# CA Network Flow Analysis

## Upgrade Guide

### Release 9.1.3

# Contact CA Technologies

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Related Documentation

CA provides a full set of technical documentation in the CA Network Flow Analysis Documentation Bookshelf. Access the bookshelf by clicking the Help link in the CA Network Flow Analysis user interface. You can open the guides in PDF and HTML format from the Documentation Bookshelf. Access the bookshelf from the Help menu in the CA Network Flow Analysis or CA Performance Center user interface.

The documentation may have been updated since its release. To be sure you have the latest documentation updates, download the bookshelf and Readme files from CA Support.

The documentation set for CA Network Flow Analysis 9.1.3 includes the following guides:

- *Online help*: Assistance for Administrators and operators, available through the Help link in the user interface.
- *Administrator Guide*: How to set up and maintain CA Network Flow Analysis.
- *Operator Guide*: How to use the NFA console to create, view, and manage reports.
- *Installation Guide*: How to install the software and perform one-time configuration tasks.
- *Upgrade Guide*: How to upgrade the software and perform initial configuration tasks.
- *Release Notes*: Summary of CA Network Flow Analysis enhancements, fixes, and open issues.
- *CA Anomaly Detector Guide:* How to install, upgrade, configure, and use CA Anomaly Detector.
- *CA Anomaly Detector Release Notes:* Overview of the product, system requirements/recommendations, and features.

The product PDFs are in the following directory: <install_path>\Reporter\NetQoS.ReporterAnalyzer.WebSite\help*<locale>*\NFA_Bookshelf\Bookshelf_Files\PDF.

To view the documentation PDF files, make sure that Adobe Reader is installed. You can download the Reader from http://get.adobe.com/reader/.

# Contents

# Chapter 1: Introduction

This guide describes how to upgrade to CA Network Flow Analysis 9.1.3.

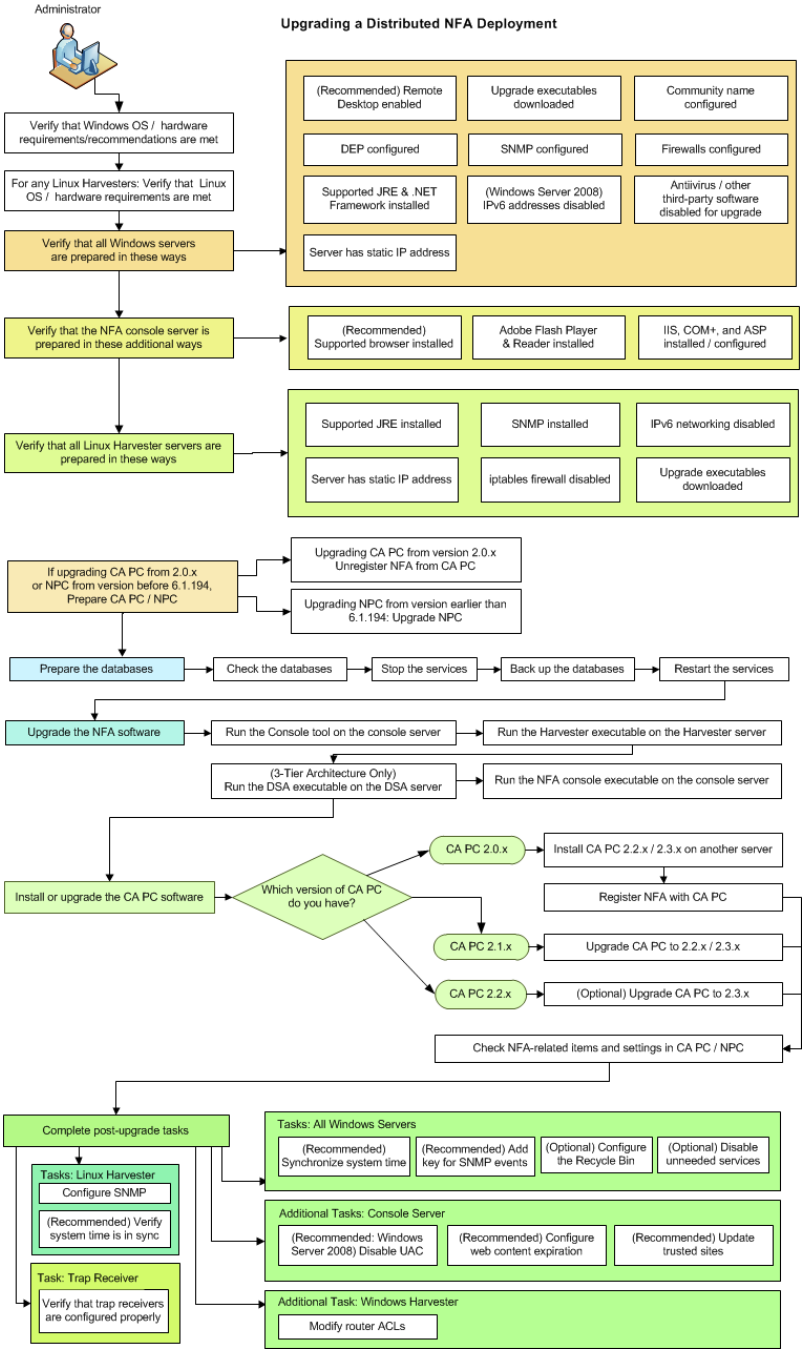
If you purchase hardware from CA Technologies, all components are delivered with the operating system and security settings already configured. Use the topics in this guide to verify the settings or update them to suit the needs of your organization.

If you purchase software only, configure and secure the operating system as described in this guide.

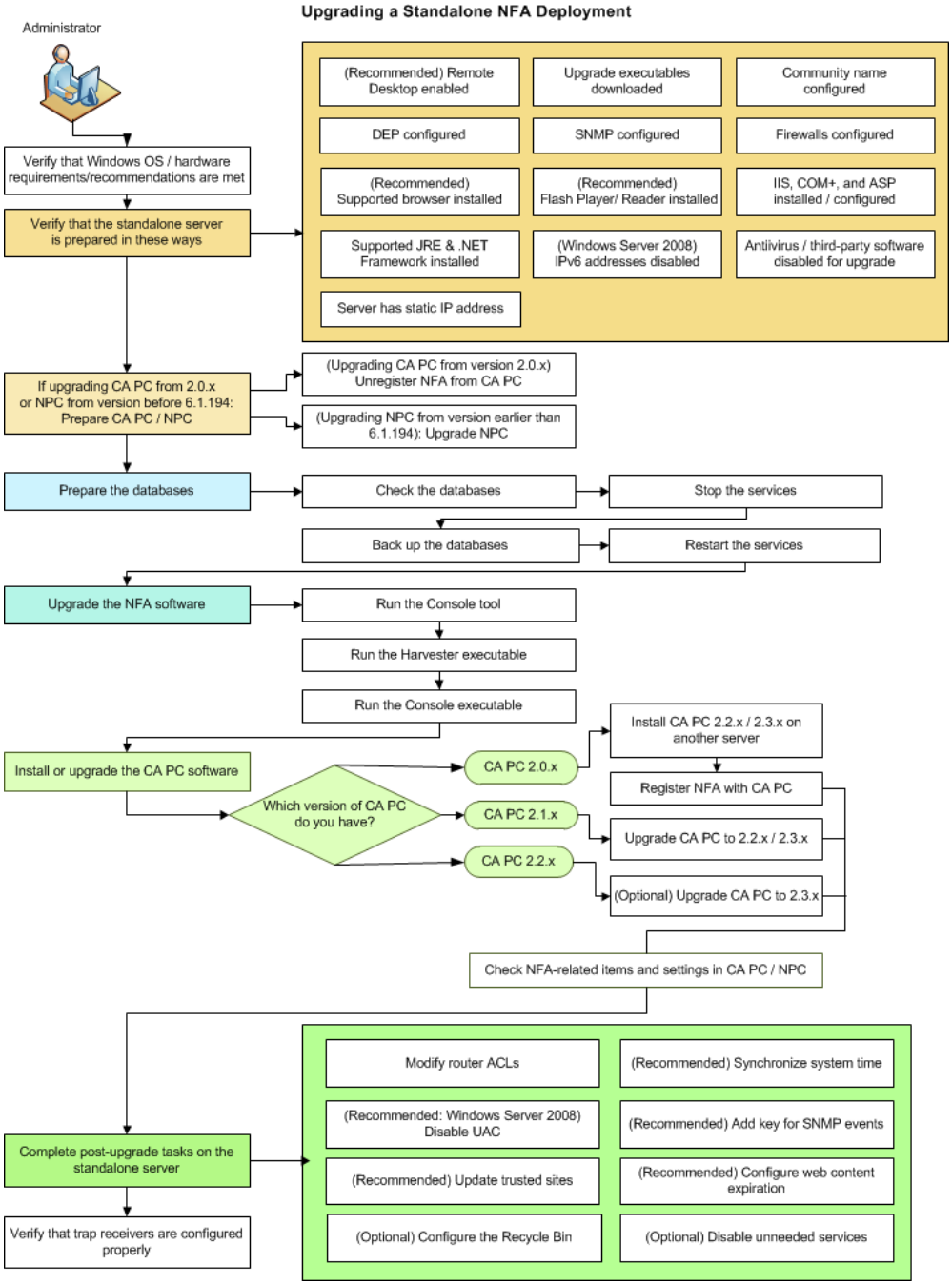
The documentation may have been updated since its release. To be sure you have the latest documentation updates, download the bookshelf and Readme files from CA Support.

The following diagrams illustrate the steps for upgrading CA Network Flow Analysis.

# Workflow for Upgrading a Distributed Deployment

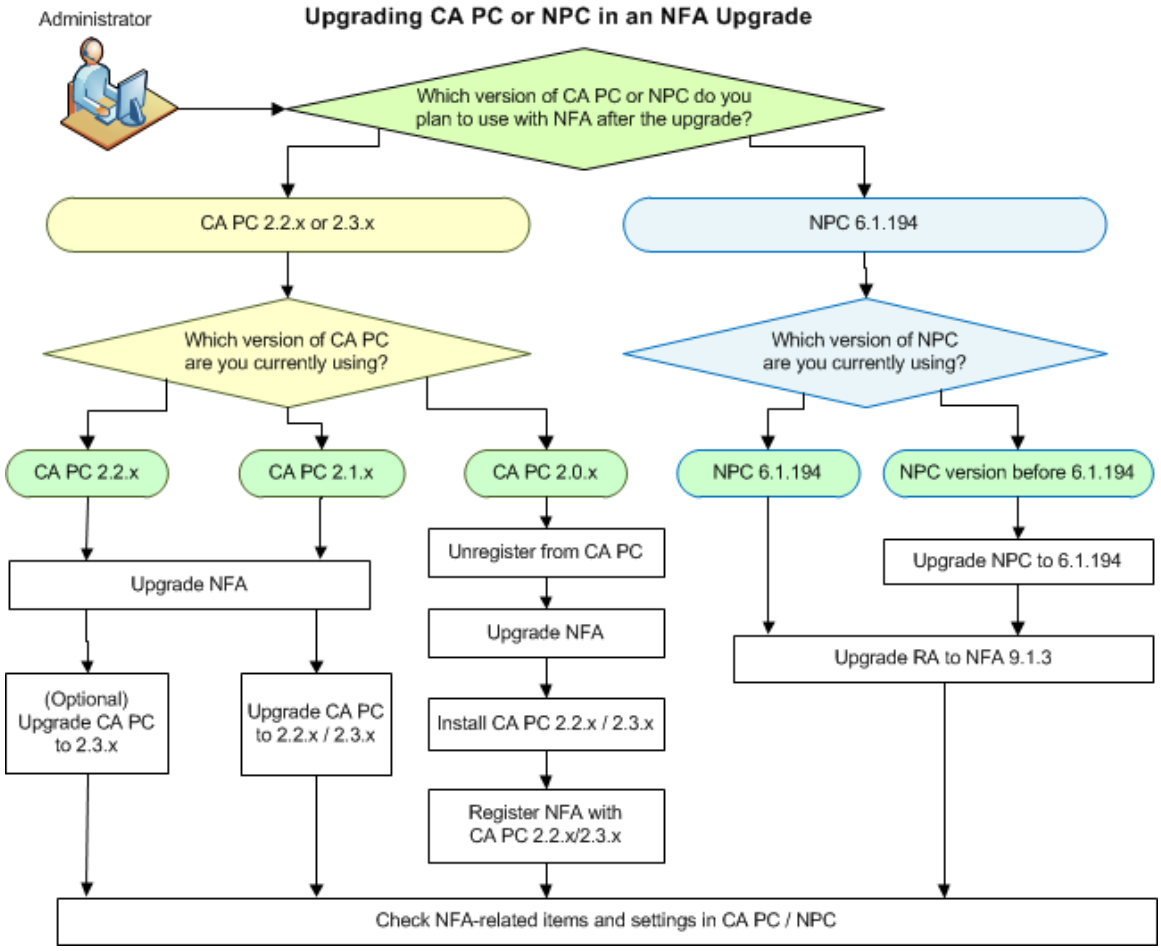


# Workflow for Upgrading a Standalone Deployment



# Workflow for Upgrading CA Performance Center or CA NetQoS Perfromance Center

The following diagram illustrates the steps for upgrading a distributed deployment of CA Network Flow Analysis.



# Software Versions That Are Supported for Upgrade

CA Network Flow Analysis 9.1.3 supports the upgrades that are described in the following table.

| FROM Version | | TO Version | |
|---|---|---|---|
| RA 9.0.161<br>NPC 6.1.194 * | Standalone 3-tier | NFA 9.1.3<br>CA PC 2.2.x,<br>CA PC 2.3.x, or<br>NPC 6.1.194 * | Standalone 2-tier |
| | Distributed 3-tier | | Distributed 3-tier |
| RA 9.1.00<br>CA PC 2.0.x * | Standalone 2-tier | NFA 9.1.3<br>CA PC 2.2.x or 2.3.x * | Standalone 2-tier |
| | Distributed 2-tier | | Distributed 2-tier |
| NFA 9.1.1<br>CA PC 2.0.x * or 2.1.x | Standalone 2-tier | NFA 9.1.3<br>CA PC 2.2.x or 2.3.x * | Standalone 2-tier |
| | Distributed 2-tier | | Distributed 2-tier |
| NFA 9.1.2<br>CA PC 2.2.x | Standalone 2-tier | NFA 9.1.3<br>CA PC 2.2.x or 2.3.x * | Standalone 2-tier |
| | Distributed 2-tier | | Distributed 2-tier |

* Your environment must include CA Performance Center 2.2.x, CA Performance Center 2.3.x, or CA NetQoS Performance Center 6.1.194. For more information about these options, see the table in Unregister from CA Performance Center (see page 37).

CA NetQoS ReporterAnalyzer 9.0.161 is the earliest software version that you can upgrade directly to CA Network Flow Analysis 9.1.3. If you have earlier software (CA NetQoS ReporterAnalyzer 8.3.16 Update 2 or 9.0), upgrade to 9.0.161 before you proceed. For more information on meeting this requirement, see the *Upgrade Instructions for ReporterAnalyzer 9.0 and 9.0 SP1* on CA Support.

**Notes:**

- Follow the recommended order for upgrading CA Network Flow Analysis and CA Performance Center or CA NetQoS Performance Center (see page 37).
- Windows NT Lan Manager (NTLM) is not supported in the current release of the Single Sign-On tool.

# Download the Installation/Upgrade Files

Copy the installation/upgrade files to the installation server so you are certain to have access to the files. Obtain the CA Network Flow Analysis installation/upgrade files from CA Technical Support, then perform one of the following tasks:

- Burn the ISO files to a CD-ROM or DVD.
- Extract the contents of the ISO files by using an ISO image software application. Many ISO image applications are free.

Extract the appropriate files to the installation servers:

- Standalone servers:
  - NFHarvesterSetup9.1.3.exe
  - RAConsoleSetup9.1.3.exe
  - consoletool-exe.jar
- Windows Harvester servers in distributed architecture deployments:
  - NFHarvesterSetup9.1.3.exe
- Linux Harvester servers in distributed architecture deployments:
  - NFHarvesterSetup9.1.3.bin
- DSA servers in three-tier distributed architecture deployments:
  - DSASetup9.1.3.exe

You can install or upgrade the software locally or remotely.

# Chapter 2: System Recommendations and Requirements

This section describes the hardware and operating system recommendations and requirements for the CA Network Flow Analysis component servers.

This section contains the following topics:



## Windows Operating System Requirements

CA Network Flow Analysis 9.1.3 supports upgrades of software versions installed on servers with the operating systems noted in the following table:

| Software Version | Operating System |
|---|---|
| From RA 9.0.161 to NFA 9.1.3 | Windows Server 2008 R2 Standard edition or Windows Server 2003 Standard edition (all components) |
| From RA 9.1.00 to NFA 9.1.3 | Windows Server 2008 R2 Standard edition (all components) |
| | Red Hat Enterprise Linux 5.5 or 5.6 (Harvester) |
| From NFA 9.1.1 to NFA 9.1.3 | Windows Server 2008 R2 Standard edition (all components) |
| | Red Hat Enterprise Linux 5.5 or 5.6 (Harvester) |
| From NFA 9.1.2 to NFA 9.1.3 | Windows Server 2008 R2 Standard edition (all components) |
| | Red Hat Enterprise Linux 5.5 or 5.6 (Harvester) |

CA Network Flow Analysis 9.1.3 supports Windows Server 2008 R2 Standard edition and Windows Server 2003 Standard edition for all components. For help upgrading your Windows operating system in preparation for the CA Network Flow Analysis upgrade, contact CA Technical Support.

If you add components on new servers to your upgraded configuration, you can install the software on servers with the following operating systems:

- Harvester:
  - Windows Server 2008 R2 Standard edition
  - Windows Server 2003 Standard edition
  - Red Hat Enterprise Linux 5.5 or 5.6
- DSA:
  - Windows Server 2008 R2 Standard edition
  - Windows Server 2003 Standard edition

The servers must meet the following requirements:

- The most recent service pack and all important updates installed
- English, Chinese (Simplified), French (France), or Japanese language

  Appropriate language packs installed on all servers for localized deployments
- Minimum display resolution of 1024x768 (XGA)
- Server configured as described in:
  - Verify Preparation of the Windows Servers (see page 21)
  - Post-Upgrade Tasks (see page 75)

**Notes:**

- Before you begin the tasks in this guide, log into a Windows server as a user who is a member of the Administrators group or into a Linux server with root privileges.
- CA Network Flow Analysis 9.1.3 supports installation on servers with IPv4 addresses. Installation is not supported at this time on servers with IPv6 addresses.
- CA Network Flow Analysis 9.1.3 supports installation and upgrade on servers with IPv4 addresses, but not IPv6 addresses.
- We recommend that you configure a single NIC (network interface card) on each server.
- The requirements and recommendations that are described in this section apply to both physical and virtual deployments.

If you have either of the following special situations, ask for help from your CA Support Availability Manager:

- DSA on Linux: Migrating Linux DSAs to Windows servers
- Changing the Installation Drive: Moving the installation location for any component to a new drive

# Hardware Recommendations for Windows Servers

In a *distributed* deployment, the CA Network Flow Analysis components are installed on separate servers.

A *standalone server* is a single server that is used for installing all of the CA Network Flow Analysis components.

We tested the product with the following hardware configuration. Your requirements may vary depending on the characteristics and volume of interfaces, applications, and operators in your network.

Notes:

- The recommended specifications described here apply to both physical and virtual deployments. The specifications represent an optimal configuration, such as the configuration of CA appliances that are currently shipping. You can run CA Network Flow Analysis successfully on configurations that do not meet these specifications, although your performance may vary.
- Performance is improved by running CA Network Flow Analysis software and the operating system on separate drives, as described in the following text. It is possible to install and run the CA Network Flow Analysis software on the same drive, however.

The following recommended specifications apply to dedicated servers that are used to install one or more CA Network Flow Analysis components:

**Standalone server**

- 2.26-GHz quad-core processor
- 3 GB RAM
- Three 146-GB 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb LAN port
- Partition for the C: drive that contains 40 GB for the operating system
- Partition for a D: drive or other separate drive that contains 41 GB for the installation/upgrade files and at least 200 GB of available space for data

**NFA console server**

- 2.26-GHz quad-core processor
- 3 GB RAM
- Three 146-GB 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb LAN port

- Partition for the C: drive that contains 40 GB for the operating system
- Partition for a D: drive or other separate drive that contains 41 GB for the installation/upgrade files and at least 200 GB of available space for data

**Harvester server**

- Two 2.26-GHz quad-core processors
- 12 GB RAM
- Six 300-GB, 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb Ethernet port
- Partition for the C: drive that contains 40 GB for the operating system
- Partition for a D: drive or other separate drive that contains 41 GB for the installation/upgrade files and 1 TB of available space for data

**Data Storage Appliance (DSA) server (3-tier architecture only)**

- 2.26-GHz quad-core processor
- 12 GB RAM
- Six 300-GB, 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb Ethernet port
- Partition for the C: drive that contains 40 GB for the operating system
- Partition for a D: drive or other separate drive that contains 41 GB for the installation/upgrade files and 1 TB of available space for data

# Linux Hardware and Operating System Recommendations and Requirements

For a distributed deployment, CA Network Flow Analysis supports running the Harvester on dedicated Linux servers that meet the following system requirements:

- Red Hat Enterprise Linux 5.5 or 5.6 on a 64-bit processor
- Java Runtime Engine (JRE) 1.6u41, which is included with the ISO files from CA Technical Support.

  If the installation server does not have JRE version 1.6 installed, the installation or upgrade program fails to launch. We recommend that you install JRE 1.6u41, the version that was used in CA Network Flow Analysis 9.1.3 testing. Untested JRE versions may produce unexpected results.
- English, Chinese (Simplified), French (France), or Japanese language

  Appropriate language packs installed on all servers for localized deployments

We recommend that Linux Harvester servers meet the following specifications:

- Two 2.26-GHz quad-core processors
- 12 GB RAM
- Six 300-GB, 10,000-RPM SAS hard drives in RAID 5 configuration
- 1-Gb Ethernet port
- Root partition that contains 40 GB of available space
- Partition for CA Network Flow Analysis that contains the following amounts of available space:
  - 41 GB for the installation/upgrade files
  - 1 TB for data

If you do not have enough available space in the /tmp directory and you cannot configure it, relocate the directory. Export the IATEMPDIR environment variable (for the Install Anywhere temporary directory) to set a new location, and select a directory with sufficient space.

**Notes:**

- CA Network Flow Analysis 9.1.3 supports installation on servers with IPv4 addresses. Installation is not supported at this time on servers with IPv6 addresses.
- The specifications described in this section apply to both physical and virtual deployments.

# Chapter 3: Preparing Windows Servers

This section contains the following topics:



## Verify Preparation of the Windows Servers

Before you begin the upgrade, verify that the following conditions are met. Failure to comply with these requirements can result in data loss, increased down time, software conflicts, or a failed upgrade.

- Verify that the installation servers have fully operational installations of CA Network Flow Analysis software that is supported for upgrade (see page 13). Verify that the correct versions of the following software are installed:
  - CA NetQoS ReporterAnalyzer or CA Network Flow Analysis components on the standalone system or distributed servers
  - CA Performance Center: Verify that the product is registered as a data source for CA Performance Center or CA NetQoS Performance Center before you upgrade. Registration is required to perform some configuration and administration tasks.

Verify that the Windows servers meet the requirements in the following table.

| Standalone Server | Distributed NFA Console Server | Distributed Harvester Server | Distributed 3-Tier DSA Server |
|---|---|---|---|
| ■ Upgrade executables are downloaded to the servers (see page 14) | | | |
| ■ Windows operating system requirements are met (see page 15) | | | |
| ■ Static IP address is assigned to each server. Set the Harvester server IP address to match the flow export destination that is assigned to each router. | | | |
| ■ Supported version of JRE and .NET Framework are installed (see page 24) * | | | |
| ■ (Recommended) Remote Desktop connection is enabled to allow remote access | | | |
| ■ (Recommended) Supported browser is installed (see page 23) ** | | | |
| ■ Firewalls are configured (see page 25) | | | |
| ■ (Recommended) Flash Player and Reader are installed (see page 24) ** | | | |
| ■ IIS, COM+, and ASP are installed [Windows Server 2008 (see page 28) or 2003 (see page 30)] ** | | | |
| ■ SNMP is configured (Windows Server 2008 (see page 32) or 2003 (see page 33)] ** | | | |
| ■ Community name is configured (see page 34) | | | |
| ■ IPv6 addresses are disabled (Windows Server 2008 systems) (see page 35) | | | |
| ■ DEP is configured (see page 36) | | | |
| ■ The following third-party software is disabled until the upgrade is complete: Antivirus, server monitoring, and maintenance software. If you enable antivirus scans later, exclude the CA Network Flow Analysis installation path and its subdirectories. | | | |
| ■ Services are stopped (see page 47), databases are backed up, and services are restarted (see page 50) | | | |

* The upgrade program either does not open or does not complete successfully unless this requirement is met.
** If the server fails to pass this check, a warning message opens.

**General Notes:**

- Stop other programs from running during the installation or upgrade.
- Restart all servers to ensure that all the installed operating system patches are applied.
- Ensure that no one else is logged in to the server during the installation or upgrade.

**Localization Notes:**

- To support non-Latin characters such as Japanese and Simplified Chinese, any command line clients that you use for installation must be configured for UTF-8 encoding. If UTF-8 encoding is not enabled, these characters may not display properly.
- The appropriate language packs are required for localized deployments.
- Regional Settings must use a period (.) to indicate a decimal value. If your deployment is localized to French, change the decimal symbol to a period in the Region and Language: Customize Format dialog.

# Supported Web Browsers

Access to the NFA console is supported for Microsoft Internet Explorer version 7 or 8. Version 8 is recommended. Other browsers or browser versions may work with CA Network Flow Analysis, but have not been tested. Microsoft Internet Explorer version 10 is not supported.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2003.<br>Windows Server 2008 R2 | NFA console server<br>Standalone server |
| Required | Windows Server 2003.<br>Windows Server 2008 R2 | Servers that are used to log into the NFA console |

**Note:** To set up CA Network Flow Analysis and work with data in the CA Performance Center Console, use Internet Explorer 8 with compatibility mode turned off. To work in CA Network Flow Analysis directly, you can use Internet Explorer 7 or 8 with compatibility mode turned on or off.

If Internet Explorer 8 Developer Tools are installed, you can turn off compatibility mode for the current browser session:

1. Press F12 on your keyboard.
2. Click the Browser Mode item on the main menu.

3. Select Internet Explorer 8.

If your enterprise has a policy that requires the Internet Explorer 8 browser to operate in compatibility mode, you may want to use Internet Explorer 7.

# Install JRE and .NET Framework

Install the following software on all of the Windows servers, logged on as a user who is a member of the Administrators group:

- Java Runtime Engine (JRE) 1.6u41, which is included with the ISO files from CA Technical Support.

  If the installation server does not have JRE version 1.6 installed, the installation or upgrade program fails to launch. We recommend that you install JRE 1.6u41, the version that was used in CA Network Flow Analysis 9.1.3 testing. Untested JRE versions may produce unexpected results.

- .NET Framework 3.5.1

  If the .NET Framework software is missing or version 4.0 is installed, a prerequisite check causes the installation or upgrade program to exit.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Required | Windows Server 2003.<br>Windows Server 2008 R2 | All servers |

# Install Adobe Applications

Adobe Flash Player is used to view reports and the Administration System Status page. We recommend that you install the latest version of Flash Player from http://get.adobe.com/flashplayer/.

Adobe Acrobat Reader is required on any system that you use to view the product documentation in PDF format. If you do not have a recent version of the Acrobat Reader, install the latest version from http://get.adobe.com/reader/.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2003.<br>Windows Server 2008 R2 | Standalone, Console |

# Firewall Configuration

For CA Network Flow Analysis to work properly in a firewall-protected environment, certain ports must be open. The following topics summarize the ports that must be open to allow communication among the CA Network Flow Analysis components. To perform these tasks, log in as a user who is a member of the Administrators group.

- Standalone system (see page 25)
- Two-tier distributed deployment (see page 26)
- Three-tier distributed deployment (see page 27)

## Ports to Open for a Standalone System

Open the following ports on a standalone system to allow CA Network Flow Analysis communications to function properly.

| From | To | Port [Function] |
|---|---|---|
| NFA console | Outbound | ■ TCP 25 [SMTP email reports]<br>■ UDP 53 [DNS] |
| Harvester | Routers (SNMP interface, read-only) | ■ UDP 161 [SNMP polling] |
| | Trap destination | ■ UDP 162 [traps] |
| Router | Harvester | ■ UDP 9995 [flow] |
| Administrators and operators | NFA console | ■ TCP/HTTP 80 [UI access and SNMP web services]<br>■ TCP/HTTP 8381 [Single Sign-On]<br>■ TCP 8681 [Report Information Base (RIB) reporting] |
| CA Performance Center Console | NFA console | ■ TCP/HTTP 80 [device and interface synchronization with CA Performance Center]<br>■ TCP 8681 [data import for CA Network Flow Analysis views in CA Performance Center] |
| Administrators | Each server | ■ TCP 3389 [Remote Desktop, if Remote Desktop is used]<br>■ TCP 5800, 5801, 5900, 5901 [VNC, if VNC is used] |

# Ports to Open for a Two-Tier Distributed Deployment

**Two-Tier Distributed Deployment**

*NFA console and Harvesters on separate servers, but no DSA*

Open the following ports in a two-tier distributed deployment to allow communication among the NFA console, Harvesters, and other elements.

| From | To | Port [Function] |
|---|---|---|
| NFA console | Outbound | ■ TCP 25 [SMTP email reports]<br>■ UDP 53 [DNS] |
| | Harvester | ■ TCP 3307 [CA MySQL]<br>■ TCP 3308 [MySQL]<br>■ TCP 8066 [SOAP web service calls]<br>■ TCP 8080 [File web server port for collecting Harvester files]<br>■ UDP 161 [Watchdog service] |
| Harvester | Routers (SNMP interface, read-only) | ■ UDP 161 [SNMP polling] |
| | Trap destination | ■ UDP 162 [traps] |
| Router | Harvester | ■ UDP 9995 [flow] |
| Administrators and operators | NFA console | ■ TCP/HTTP 80 [UI access and SNMP web services]<br>■ TCP/HTTP 8381 [Single Sign-On]<br>■ TCP 8681 [Report Information Base (RIB) reporting] |
| CA Performance Center Console | NFA console | ■ TCP/HTTP 80 [device and interface synchronization with CA Performance Center]<br>■ TCP 8681 [data import for CA Network Flow Analysis views in CA Performance Center] |
| Administrators | Each server | ■ TCP 3389 [Remote Desktop, if Remote Desktop is used]<br>■ TCP 5800, 5801, 5900, 5901 [VNC, if VNC is used] |

## Ports to Open for a Three-Tier Distributed Deployment

**Three-Tier Distributed Deployment**

*NFA console, Harvester, and DSA components on separate servers*

Open the following ports in a three-tier distributed deployment to allow communication among the NFA console, Harvesters, DSAs, and other elements.

| From | To | Port [Function] |
|---|---|---|
| NFA console | Outbound | ■ TCP 25 [SMTP email reports]<br>■ UDP 53 [DNS] |
| | Harvester | ■ TCP 3307 [CA MySQL]<br>■ TCP 3308 [MySQL]<br>■ TCP 8066 [SOAP web service calls]<br>■ TCP 8080 [File web server port for collecting Harvester files]<br>■ UDP 161 [Watchdog service] |
| | DSA | ■ TCP 3307 [CA MySQL]<br>■ TCP 3308 [MySQL]<br>■ UDP 161 [Watchdog service] |
| Harvester | Routers (SNMP interface, read-only) | ■ UDP 161 [SNMP polling] |
| | Trap destination | ■ UDP 162 [traps] |
| DSA | NFA console | ■ TCP 3308 [MySQL]<br>■ TCP 8080 [File Web Service, which retrieves files from the NFA console without using a file share] |
| Router | Harvester | ■ UDP 9995 [flow] |
| Administrators and operators | NFA console | ■ TCP/HTTP 80 [UI access and SNMP web services]<br>■ TCP/HTTP 8381 [Single Sign-On]<br>■ TCP 8681 [Report Information Base (RIB) reporting] |
| CA Performance Center Console | NFA console | ■ TCP/HTTP 80 [device and interface synchronization with CA Performance Center]<br>■ TCP 8681 [data import for CA Network Flow Analysis views in CA Performance Center] |

| From | To | Port [Function] |
|---|---|---|
| Administrators | Each server | ■ TCP 3389 [Remote Desktop, if Remote Desktop is used]<br>■ TCP 5800, 5801, 5900, 5901 [VNC, if VNC is used] |

# Install IIS, ASP, and COM+

To run the CA Network Flow Analysis software successfully on a standalone server or NFA console server, install Internet Information Services (IIS), ASP, and COM+ as described in the related topics for:

- Windows Server 2008 R2 (see page 28)
- Windows Server 2003 (see page 30)

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Required | Windows Server 2003,<br>Windows Server 2008 R2 | Standalone, Console |

## Install IIS, ASP, and COM+ on Windows Server 2008 R2

Use the steps in this topic to install the following required components on a standalone server or NFA console server that is running Windows Server 2008 R2:

- IIS
- ASP
- IIS 6 Management Compatibility
- COM+ Network Access

**Follow these steps:**

1. Log in to the server as a user who is a member of the Administrators group.
2. Select Start, Administrative Tools, Server Manager.

   The Server Manager window opens.
3. Expand the Roles list in the Console tree on the left.

4. Add the IIS role service:
    a. Click the Application Server link under Roles in the Console tree on the left.

       The Application Server view opens in the right pane.

    b. Click the Add Role Services link in the Role Services section.

       The Add Role Services wizard opens to the Select Role Services page.

    c. Select the Web Server (IIS) Support check box.

       A confirmation message appears.

    d. Click Add Required Role Services in the confirmation message.

       The Web Server (IIS) Support option is highlighted on the Select Role Services page.

5. Add the COM+ role service:
    a. Select the COM+ Network Access check box.

       A confirmation message appears.

    b. Click Add Required Role Services in the confirmation message, then click Next.

       The Web Server (IIS) page of the Add Role Services wizard opens.

6. Enable IIS 6 Management Compatibility:
    a. Click Next again.

       A list of role services appears in the wizard.

    b. Select the IIS 6 Management Compatibility check box in the Management Tools section of the list, then click Next.

       The Confirm Installation Selections page summarizes your actions and displays related messages.

7. Install the IIS and COM+ role services and options you selected:
    a. Click Install.

       The Progress page is shown until the installation or upgrade is complete, when the Results page opens.

    b. (Optional) Click 'Print, e-mail, or save the installation/upgrade report, review the information,' then close the page.

       The Installation Report page displays a summary of your changes, information about the changes, and the location of the full installation/upgrade log.

    c. Click Close.

       The Results page closes.

8. Add and install the ASP role service:
    a. Click the Web Server (IIS) link under Roles in the Console tree on the left.

       The Web Server (IIS) view opens in the right pane.

    b. Click the Add Role Services link in the Role Services section.

       The Add Role Services wizard opens to the Select Role Services page.

    c. Select the ASP check box under Application Development in the list and click Next.

       The Confirm Installation Selections page summarizes your actions and related messages.

    d. Click Install.

       The Progress page is shown until the installation or upgrade is complete, when the Results page opens.

    e. (Optional) Click 'Print, e-mail, or save the installation/upgrade report, review the information,' then close the page.

       The Installation Report page displays a summary of your changes, information about the changes, and the location of the full installation/upgrade log.

    f. Click Close.

       The Installation Results page closes.
9. Exit from the Server Manager window.

## Install IIS, ASP, and COM+ on Windows Server 2003

Use the steps in this topic to install the following required components on a standalone server or NFA console server that is running Windows Server 2003:

- ASP.NET
- Network COM+ access
- Internet Information Services (IIS)
  with the Active Server Pages option enabled for the World Wide Web service

**Follow these steps:**

1. Log in to the server as a user who is a member of the Administrators group.
2. Open the Windows Component wizard:
    a. Select Start, Control Panel, Add or Remove Programs.

       The Add or Remove Programs window opens.

    b. Click Add/Remove Windows Components in the left pane.

       The Windows Components Wizard window opens.

3. Select the components to add:
   a. Select Application Server in the list.
   b. Click Details.

      The Application Server dialog opens and displays a list of optional Application Server components.
   c. Select the following check boxes:
      - ASP.NET check box.
      - Enable network COM+ access (selected automatically when you select ASP.NET)
      - Internet Information Services (IIS) (selected automatically when you select ASP.NET)
4. Select the Active Server Pages subcomponent to be enabled for the World Wide Web service:
   a. Select Internet Information Services (IIS) in the Application Server component list.
   b. Click Details.

      The Internet Information Services (IIS) dialog opens and displays a list of optional IIS subcomponents.
   c. Highlight the World Wide Web Service subcomponent. This check box is selected by default.

      The World Wide Web Service dialog opens and shows a list of subcomponents.
   d. Select the Active Server Pages (ASP) check box.
5. Save your selections:
   a. Click OK in the World Wide Web Service dialog.

      You return to the Internet Information Services (IIS) dialog.
   b. Click OK in the Internet Information Services (IIS) dialog.

      You return to the Application Server dialog.
   c. Click OK in the Application Server dialog.

      You return to the Windows Component Wizard.

6. Update the Windows configuration with your selections:
   a. Click Next in the Windows Components Wizard screen.

      The system locates the files for the update. If any files are missing, a message opens. In this case, insert the Windows 2003 Server Edition CD-ROM or specify the path to the missing files.

      A message notifies you when the preparations are complete.

   b. Click Finish.

      The Windows Components wizard closes. The Windows configuration changes are complete.

# Configure SNMP

The Simple Network Management Protocol (SNMP) service is required by the Watchdog services. Configure the SNMP service as described in the related topics for:

- Windows Server 2008 R2 (see page 32)
- Windows Server 2003 (see page 33)

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Required | Windows Server 2003, Windows Server 2008 R2 | All servers |

## Configure SNMP on Windows Server 2008 R2

Use the steps in this topic to configure the SNMP service as required on all Windows Server 2008 R2 servers in your CA Network Flow Analysis deployment.

**Follow these steps:**

1. Log in to the server as a user who is a member of the Administrators group.
2. Select Start, Administrative Tools, Server Manager.

   The Server Manager window opens.
3. Click Features in the left pane.

   The Server Manager window displays a list of the installed features.
4. Click Add Features in the right pane.

   The Add Features wizard opens and shows the list of selected and available features.

5. Select the SNMP Services check box in the list.

   A confirmation message appears.

6. Click Add Required Features.

   The Confirm Installation Services page identifies the features to be installed. The page also displays important messages about the installation or upgrade.

7. Click Install.

   The Installation Progress page opens. When the installation or upgrade is complete, the Installation Results page opens, identifies the new features, and indicates whether you will need to restart the server.

8. Click Close.

   A message asks whether you want to restart the server now.

9. Click Yes.

   After the server restarts, the Features view in the Server Manager window shows the newly installed feature.

## Configure SNMP on Windows Server 2003

Use the steps in this topic to configure the SNMP service as required on all Windows Server 2003 servers in your CA Network Flow Analysis deployment.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Open the Windows Component wizard:
   a. Select Start, Control Panel, Add or Remove Programs.

      The Add or Remove Programs window opens.

   b. Click Add/Remove Windows Components in the left pane.

      The Windows Components Wizard window opens.
3. Add Simple Network Management Protocol (SNMP):
   a. Highlight Management and Monitoring Tools in the Windows Component Wizard component list and click Details.

      The Management and Monitoring Tools dialog opens.

   b. Select the Simple Network Management Protocol check box.

   c. Click OK.

      The Management and Monitoring Tools dialog closes and you return to the Windows Components Wizard screen. SNMP is set to be added.

4. Update the Windows configuration with your selections:
   a. Click Next in the Windows Components Wizard screen.

      The system locates the files for the update. If any files are missing, a message opens. In this case, insert the Windows 2003 Server Edition CD-ROM or specify the path to the missing files.

      A message notifies you when the preparations are complete.

   b. Click Finish.

      The Windows Components wizard closes. The selected components are added to your Windows configuration.

# Configure the SNMP Community Name

Define the community name for the SNMP service to help prevent polling errors and help product components work properly. Use the same community name that is defined on the Watchdog Settings page, which is "public" by default. This topic describes how to define the community name as "public" on a Windows server in your CA Network Flow Analysis deployment.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Required | Windows Server 2003,<br>Windows Server 2008 R2 | All servers |

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Select Start, Administrative Tools, Services.

   The Services window opens.
3. Right-click the SNMP Service and select Properties.

   The SNMP Service Properties dialog opens.
4. Select the Security tab.
5. Verify that the appropriate community name is in the "Accepted community names" list. The default community name is "public."
6. If the appropriate community name is not listed, add it:
   a. Click Add.

      The SNMP Service Configuration dialog opens.

   b. Set the following options:
      - Community rights: Select Read Only.

- Community Name: Enter **public** or a custom community name. Use the same community name throughout the CA Network Flow Analysis deployment:

  snmpd.conf file on each Linux server

  SNMP service on each Windows server

  Watchdog Settings page of the NFA console

c. Click Add.

   The SNMP Service Configuration dialog closes. The SNMP Service Properties dialog displays the new name in the "Accepted community names" list.

7. Click OK in the SNMP Service Properties dialog.

   Any changes that you made are saved. The SNMP Service Properties dialog closes.

8. Select File, Exit in the Services window.

   The Services window closes.

# Disable Connections to IPv6 Addresses on Windows Server 2008 R2

We recommend that you set up Windows Server 2008 R2 systems so that they are prevented from connecting to IPv6 addresses, which are currently not supported. If connection to IPv6-formatted addresses is enabled, data collection fails. This topic describes how to perform this task on the Windows Server 2008 R2 systems in your CA Network Flow Analysis deployment.

**Note:** Windows Server 2003 systems disable connection to IPv6 addresses by default. You do not need to perform this task on a Windows Server 2003 system unless the "Microsoft TCP/IP version 6" option has been enabled for network connections.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2008 R2 | All servers |

The instructions are based on the assumption that each server has a single network interface card, which is the recommended configuration.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Open the Network Connections window:
   a. Select Start, Control Panel.
   b. Click Network and Internet in the Control Panel.

c. Click Network and Sharing Center in the Network and Internet window that opens.

d. Click "Change adapter settings" on the left side of the Network and Sharing Center window that opens.

   The Network Connections window opens and shows the currently configured connections.

3. Right-click the connection.
4. Select Properties from the menu.

   The Properties dialog opens.

5. Clear the check box labeled 'Internet Protocol Version 6 (TCP/IPv6),' if it is selected.
6. Click OK.

   Any changes that you made are saved. The Properties dialog box closes,

7. Select Organize, Close in the Network Connections window.

   The Network Connections window closes.

# Configure Data Execution Prevention (DEP)

Data Execution Prevention (DEP) helps to prevent code execution from data pages. This topic describes how to configure the appropriate DEP policy level on a Windows Server 2008 R2 system.

A Windows Server 2003 system should have the appropriate setting enabled by default unless a different policy level is specified in an unattended installation. If the default OptIn DEP policy level has been overridden on your Windows Server 2003 system, consult the Microsoft support site for steps to restore the setting.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Required | Windows Server 2003,<br>Windows Server 2008 R2 | All servers |

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Open the Control Panel and click the System link.
3. Click the Advanced tab in the System Properties dialog that opens.
4. Click Settings.

5. Click the Data Execution Prevention tab in the Performance Options dialog that opens.
6. Select "Turn on DEP for essential Windows programs and services only."
7. Save your settings and exit:
   a. Click OK in the Performance Options dialog.

      Your settings are saved and the dialog closes.

   b. Click OK in the System Properties dialog.

      A message opens and informs you that you must restart your system to make the new settings take effect.
8. (Optional) Restart your system before you install or upgrade the software.

   If you proceed with software installation or upgrade without restarting the system, the prerequisite test displays a warning about your DEP configuration.

# Unregister from CA Performance Center

The NFA console or standalone server must be registered as a data source with a supported version of CA Performance Center or CA NetQoS Performance Center. Your next step depends on your current software version and the version you want to use after the upgrade, as described in the following table.

Many customizations are lost when you unregister and register again. Read this topic carefully to prepare for these events.

### General Guidelines:

- If you need to unregister, complete the steps in this topic before you start the CA Network Flow Analysis upgrade.
- Upgrade CA Network Flow Analysis first if you need to upgrade the following software:
  - CA NetQoS Performance Center from 6.1.x to 6.1.194
  - CA Performance Center 2.1.x to CA Performance Center 2.2.x, then optionally to version 2.3.x
  - CA Performance Center 2.2.x to CA Performance Center 2.3.x

| Pre-Upgrade Version | Post-Upgrade Version | Upgrade Order |
|---|---|---|
| NFA 9.1.2,<br>CA PC 2.2.x | NFA 9.1.3,<br>CA PC 2.2.x or 2.3.x | 1) Upgrade NFA.<br>2) Check NFA-related items and settings in CA PC. |
| NFA 9.1.1,<br>CA PC 2.1.x | | 1) Upgrade NFA.<br>2) Upgrade CA PC as described in the *CA Performance Center Installation Guide.* |
| NFA 9.1.1,<br>CA PC 2.0.x | | 1) Unregister as a data source (see page 37).<br>2) Upgrade NFA.<br>3) Register with CA PC (see page 77).<br>4) Check NFA-related items and settings in CA PC. |
| NFA 9.1.00,<br>CA PC 2.0.x | | |
| RA 9.0.161,<br>NPC 6.1.x | | |
| RA 9.0.161,<br>NPC 6.1.194 | NFA 9.1.3,<br>NPC 6.1.194 | 1) Upgrade NFA<br>2) Check NFA-related items and settings in NPC. |
| RA 9.0.161,<br>NPC 6.1, build that pre-dates 194 | | 1) Upgrade NPC to version 6.1.194, as described in the *CA NetQoS Performance Center Installation Guide.*<br>2) Upgrade NFA<br>3) Check NFA-related items and settings in NPC. |

You can upgrade to CA Performance Center 2.2.x or 2.3.x incrementally from version 2.1.x, but you cannot upgrade to version 2.2.x or 2.3.x from 2.0.x or an earlier version.

We generally do not recommend unregistering. We recommend that you unregister only when you cannot upgrade to the CA Performance Center version that you want to use.

**Results of Unregistering:**

If you unregister CA Network Flow Analysis from CA Performance Center 2.0.x or CA NetQoS Performance Center 6.1 and register it again with CA Performance Center 2.2.x or 2.3.x, the following rules apply:

- Domains:
  - The default domain is retained. Groups, users, devices (routers), interfaces, protocol names, and ToS labels that are assigned to the default domain retain their assignments.
  - Custom domains are deleted.
  - Groups, users, devices (routers), and interfaces in custom domains are reassigned to the default domain.

- Protocol names, ToS labels, AS names, and IP addresses in custom domains become inaccessible.

- User accounts:
  - User accounts are retained if the users have valid product privilege settings (User, Power User, or Administrator) for CA Network Flow Analysis. User accounts with no product privilege for CA Network Flow Analysis are deleted.
  - User accounts that are associated with custom domains will be associated with the default domain instead.
  - If the user account 'nqadmin' exists and has a product privilege that is lower than Administrator, this user account acquires the Administrator product privilege.

  You cannot add new users or edit user account settings after you unregister.

- Roles:
  - Custom and default roles are retained and continue to be associated with user accounts.

- Groups: Retained if the following conditions are met:
  - The group is a default group in CA NetQoS Performance Center or is a group that was pushed up to CA NetQoS Performance Center. 'Dynamic groups,' for example, cross-product groups, are deleted.
  - The group has contents--that is, the group is not empty.

  Custom and default groups require cleanup on the Manage Groups page in CA Performance Center after you unregister and register with the newer software. The following changes may occur:

  - Some group names change slightly. For example, the group 'All Interfaces' is renamed 'Interfaces.'
  - Structures may flatten so that a group that was nested under another group is not nested.
  - Groups may be relocated:

    A custom group that originally was shown on the Manage Groups page under All Groups/System Groups/Data Sources/ReporterAnalyzer is under Network Flow Analysis in the new group tree. The new location is All Groups/Inventory/Data Sources/Network Flow Analysis.

    If the custom group originally was not under ReporterAnalyzer, it is moved to sit under Network Flow Analysis.

  - Duplicate groups may be created.
  - Empty custom groups are deleted.

- SNMP profiles: SNMP profiles from NetQos Performance Center 6.1.194 are retained with no changes in their status.

- Single Sign-On (SSO) customizations: LDAP and other SSO customizations are retained.

  **Note:** If you upgrade from CA NetQoS ReporterAnalyzer 9.0.1, you also will change to a new SSO version. Update any previous SSO LDAP configuration and check other SSO customizations. Options from the previous SSO version may not match the current options or may not comprise a full set of the current options. For information about configuring SSO, see the *Single Sign-On User Guide*.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Review your records of the customizations in CA NetQoS Performance Center or CA Performance Center, such as:
   - User accounts and their roles, product permissions, groups, and domain access
   - Custom roles and standard roles that have been customized, including any assignments for top-level menus, dashboards, and dashboard menus
   - Group structure and naming conventions
   - Custom domains and their contents, such as groups, devices, interfaces, SNMP profiles, report folders, AS names, protocol names, ToS labels, and IP addresses

   Remember that these elements may require checking, restructuring, or restoration.
3. Open the Data Source List: Click Admin, NetQoS Settings group, Data Sources.
4. Select the Reporter Analyzer or CA Network Flow Analysis data source.
5. Click Delete.

# Chapter 4: Preparing Linux Servers

This section contains the following topics:



## Verify Preparation of the Linux Servers

Before you begin the upgrade, verify that the following conditions are met. Failure to comply with these requirements can result in data loss, increased down time, software conflicts, or a failed upgrade.

- System Requirements: Verify that the upgrade servers meet the Linux requirements and recommendations (see page 19).
- Software Requirements: Verify that the upgrade servers have fully operational CA Network Flow Analysis software that is supported for upgrade (see page 13).
- Verify that each of the Harvester Linux servers is ready for the upgrade by:
  - Installing the supported JRE version:  Java Runtime Engine (JRE) 1.6u41.
  - Assigning a static IP address to each server. Set the Harvester server IP address to match the flow export destination that is assigned to each router.
  - Configuring SNMP (see page 42)

    If SNMP is not running, the upgrade program displays a warning. You can bypass the warning and configure SNMP after the upgrade, however.
  - Disabling the iptables firewall (see page 43)
  - Disabling IPv6 networking (see page 43)
  - Stopping services (see page 49)
  - Backing up the databases (see page 50)

- To support non-Latin characters such as Japanese and Simplified Chinese, any command line clients that you use for installation must be configured for UTF-8 encoding. If UTF-8 encoding is not enabled, these characters may not display properly.
- The appropriate language packs are required for localized deployments.
- Regional Settings must use a period (.) to indicate a decimal value. If your deployment is localized to French, change the decimal symbol to a period in the Region and Language: Customize Format dialog.
- Polling fails if DNS resolution is not configured. For more information, see the Readme.

# Install SNMP on Linux Servers

To configure a Linux server for a Harvester, complete the following main tasks:

- If Net-SNMP if it is not already present on the installation or upgrade server, install it as described in this topic.
- Finish SNMP configuration after the installation or upgrade is complete: (see page 80)
  - Set up the Net-SNMP configuration file.
  - Configure SNMP to start automatically on boot.
  - Start the snmpd service.

Verify that Net-SNMP is present on the server and install it if necessary. Net-SNMP is required to support Watchdog functionality.

**Follow these steps:**

1. Open the Linux Package Manager and look for listings that contain "net-snmp."

   If you do not find any "net-snmp" listings, Net-SNMP is not installed.
2. Get and install Net-SNMP if it is not installed. For example, you can get Net-SNMP from the Linux Package Manager.

# Disable the iptables Firewall for Linux Servers

We recommend that you disable the iptables firewall and stop the iptables service on each Linux server that has a Harvester installed. Disabling iptables ensures that all the required ports are open and that the iptables firewall does not impact performance adversely.

**Note:** If your enterprise requires the use of iptables, make sure that you open all of the applicable firewall ports in the firewall configuration list (see page 25). In addition make sure that you have full localhost-to-localhost access. This step is required because CA Network Flow Analysis uses RMI (Remote Method Invocation) access.

Complete the following steps to disable all levels of iptables and allow communication among CA Network Flow Analysis components.

**Follow these steps:**

1. Log in as root or with a sudo user account.
2. Run the following commands in a command prompt window:

   ```
   service iptables stop

   chkconfig iptables off

   chkconfig –-list |grep iptables
   ```

3. Review the output of the last command to make sure that all of the iptables levels are off, as shown in the following example:

   ```
   iptables 0:off 1:off 2:off 3:off 4:off 5:off 6:off
   ```

# Disable IPv6 Networking on Linux Servers

Disable IPv6 networking on each Linux server that has a Harvester installed.

**Note:** Complete this task before you add the Harvester in the NFA console. If IPv6 is enabled when you add a Harvester in the NFA console, the Harvester automatically binds with an IPv6-format address, which prevents CA Network Flow Analysis from receiving its data.

To disable IPv6 networking, modify the following files:

- Kernel driver configuration file, modprobe.conf, which is located by default in the /etc directory
- RHEL networking configuration file, network, which is located by default in the /etc/sysconfig directory

**Follow these steps:**

1. Make sure that you are logged in with root privileges.
2. Edit the modprobe.conf file:
   a. Open the /etc/modprobe.config file in a text editor.
   b. Append the following line:
      `install ipv6 /bin/true`
   c. Save and close the file.

      The modprobe.conf file is now configured so that when the system attempts to load the IPv6 kernel module, it executes the command 'true' instead of loading the module. The 'true' command performs no action.
3. Edit the network file:
   a. Open the /etc/sysconfig/network file in a text editor.
   b. Update or add the following lines to match the text strings shown:
      `NETWORKING_IPV6=no`
      `IPV6INIT=no`
   c. Save and close the file.
4. Reboot the server:
   `reboot`
5. Verify that IPv6 is disabled:
   a. Enter the following command at a terminal:
      `lsmod | grep ipv6`

      If the command returns no output, the IPv6 kernel module is not running: It has been removed successfully.
   b. Enter the /sbin/ifconfig command:
      `/sbin/ifconfig`

      Check the output to verify that it contains only IPv4 addresses and no IPv6 addresses.

# Chapter 5: Check and Back Up the Databases

This section contains the following topics:



## Check the MySQL Databases

When you upgrade to CA Network Flow Analysis 9.1.3, the data from several MySQL databases is migrated after the software upgrade is complete. Data migration consists of saving the data to newly formatted MySQL database tables. Data migration may be a lengthy process, which is likely to fail if any of the existing database tables are corrupt.

We recommend that you check the database tables before migration to correct problems in database tables, avoid a migration failure, and avoid stepping through recovery assistance with CA Support. This topic describes how to run the mysqlcheck command before the upgrade to verify that the database tables are set up properly for migration.

You can run the mysqlcheck command to check the following pre-upgrade databases:

- reporter:* Located on each standalone or NFA console server (upgrade from 9.0.1, 9.1.00, or 9.1.1)
- harvester: Located on each standalone or Harvester server (upgrade from 9.0.1, 9.1.00, or 9.1.1)
- poller: Located on each standalone or Harvester server (upgrade from 9.1.00 or 9.1.1)
- data_retention: Located on each CA Network Flow Analysis component server (upgrade from 9.1.00 or 9.1.1)
- nqrptr:* Located on each DSA server (upgrade from 9.0.1)

  * Database that typically contains some large tables

Checking large database tables can be time-consuming. If you run the check on an entire database, each table in the database is locked in read-only state and is unavailable for write operations. If you run the check on single tables, the other tables in the database remain write-accessible.

You can run mysqlcheck without stopping MySQL: The MySQL deamon process (mysqld) can continue to run on Linux servers and the MySQL service can continue to run on Windows servers.

**Follow these steps:**

1. Log in to one of the CA Network Flow Analysis servers as a user with administrator privileges. On a Linux Harvester server, log in as root.

   Upgrade from 9.0.1:

   - Standalone server: Check the harvester, reporter, and nqrptr databases.
   - Harvester server (distributed deployment): Check the harvester database.
   - NFA console server (distributed deployment): Check the reporter database.
   - DSA server (distributed deployment): Check the nqrptr database.

   Upgrade from 9.1.00 or 9.1.1:

   - Standalone server: Check the harvester, reporter, poller, and data_retention databases
   - Harvester server (distributed deployment): Check the harvester, poller, and data_retention databases
   - NFA console server (distributed deployment): Check the reporter database

2. Enter one of the following mysqlcheck commands at a command or shell prompt:

   - To check the tables in all of the applicable databases on the server:

     ```
     mysqlcheck --all-databases
     ```

   - To check all of the tables in a single database:

     ```
     mysqlcheck --databases db_name
     ```

     **Example**:

     ```
     mysqlcheck --databases reporter
     ```

   - To check a single database table:

     ```
     mysqlcheck db_name [tbl_name]
     ```

     **Example**:

     ```
     mysqlcheck reporter [reporter.harvesters]
     ```

   where:

   db_name = Name of the database that you want to check

   tbl_name = Name of any table that you want to check individually in a database

You do not need to specify the path to the database. The mysqlcheck command will find any or all databases that use the default port (port 3308). The custom storage engine does not support the use of the mysqlcheck command for its archive and archive15 databases. The command fails to run even if you specify the correct port (port 3307) for the connection to these databases.

The command checks each table, attempts to repair any problems, then analyzes and optimizes the table. The command returns a list of the database tables that were checked and reports the status for each table.

If the table passed the check, "OK" follows the table name. If a warning is returned and is followed by "OK," the problem was resolved. If unresolved errors occur, contact CA Support.

**Next:** Stop the services, then back up the databases, as described in the following topics.

# Stop the Services

Before you back up the databases and upgrade the CA Network Flow Analysis software, prevent new data from being sent to the NFA console until the upgrade is complete. Failure to stop the services does not cause the upgrade to fail, but some collected data is not processed.

## Stop Services on Windows Servers

To prepare for backing up the databases, stop the services on all of the Windows servers in your CA Network Flow Analysis deployment.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Open the Services window: Click Start, Control Panel, Administrative Tools, Services.
3. Stop the Harvester service (NetQoS Harvester service or CA NFA Harvester) on each Harvester server.
4. Wait 15 minutes for data file processing to complete.

5. Stop the ReporterAnalyzer or CA Network Flow Analysis services on each Windows server:

   - If you are upgrading a ReporterAnalyzer 9.0.1 deployment, stop the following services:

| 9.0.1 Service | Standalone | Harvester | Console | DSA |
|---|---|---|---|---|
| NetQoS Management Server | Yes | Yes | | |
| NetQoS MySql51 | Yes | Yes | Yes | Yes |
| NetQoS NQMySql51 | Yes | Yes | | |
| NetQoS Reaper | Yes | Yes | | |
| NetQoS ReporterAnalyzer DSA Loader Service | Yes | | | Yes |
| NetQoS Reporter/Analyzer General Services | Yes | | Yes | |
| NetQoS Reporter/Analyzer Pump Service | Yes | | Yes | |
| NetQoS Reporter/Analyzer Query Services | Yes | | Yes | |
| NetQoS Reporter/Analyzer Report Service | Yes | | Yes | |
| NetQoS Reporter/Analyzer Watchdog | Yes | | Yes | |
| NetQoS Reporter Manager Service | Yes | | Yes | |

   - If you are upgrading a CA Network Flow Analysis 9.1.00 or 9.1.1 deployment, stop the following services:

| 9.1.00 or 9.1.1 Service | Standalone | Harvester | Console |
|---|---|---|---|
| CA NFA Collection and Poller Webservices | Yes | Yes | |
| CA NFA DMS/SNMP Proxies | Yes | Yes | Yes |
| CA NFA Harvester Data Retention | Yes | Yes | |
| CA NFA Harvester File Pump Web Service | Yes | Yes | |
| CA NFA Poller | Yes | Yes | |
| CA NFA Reaper | Yes | Yes | |
| CA NFA RibSource | Yes | | Yes |
| NetQoS MySql51 | Yes | Yes | Yes |
| NetQoS NQMySql51 | Yes | | Yes |
| NetQoS Reporter Manager Service | Yes | | Yes |

| 9.1.00 or 9.1.1 Service | Standalone | Harvester | Console |
|---|---|---|---|
| NetQoS Reporter/Analyzer General Services | Yes | | Yes |
| NetQoS Reporter/Analyzer Pump Service | Yes | | Yes |
| NetQoS Reporter/Analyzer Query Services | Yes | | Yes |
| NetQoS Reporter/Analyzer Report Service | Yes | | Yes |
| NetQoS Reporter/Analyzer Watchdog | Yes | | Yes |

The services and data collection stop. The data files are processed within 15 minutes.

6. Check the following directory on the NFA console server:

   <install_path>\Netflow\datafiles\HarvesterWork

   When the HarvesterWork folder is empty, you can back up the database.

   The services are restarted automatically during the upgrade process.

## Stop Services on Linux Servers

To prepare for the database backups, stop the services on any Linux Harvester servers that are in your product deployment.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Stop the nfa_harvester (CA NFA Harvester) service on each Linux Harvester server.
3. Wait 15 minutes for data file processing to complete.
4. Stop the following services on each Linux Harvester server:
   - mysql51 (NetQoS MySQL51)
   - nfa_collpollws (CA NFA Collection and Poller Webservices)
   - nfa_dataretention (CA NFA Data Retention)
   - nfa_filewebservice (CA NFA File Server) (if upgrading from NFA 9.1.2)
   - nfa_mysqlCSE (NetQoS NQMySql51 Custom Storage Engine)
   - nfa_poller (CA NFA Poller)
   - nfa_proxies (CA NFA DNS/SNMP Proxies)
   - nfa_reaper (CA NFA Reaper)

   After you stop the services, the Time BIN (.tbn) files are collected and processed within 15 minutes.

5. Check the following directory on the NFA console server:
<install_path>\Netflow\datafiles\HarvesterWork

   When the HarvesterWork folder is empty, you can back up the database.

   The services are restarted automatically during the upgrade process.

# Back Up the Databases and Restart the Services

The next step is to back up the CA Network Flow Analysis or ReporterAnalyzer databases.

## Back Up 9.0.1 Databases

Before you upgrade a CA Network Flow Analysis 9.0.1 deployment, back up the databases and files that are listed in the following table.

| Database | Description | Standalone Server | Harvester Servers (Distributed) | NFA Console Server (Distributed) |
|---|---|---|---|---|
| reporter | Enterprise Overview data and NFA console configuration data | Important | | Important |
| harvester | Harvester configuration data | Important | Important | |
| nqrptr | Historical (15-minute) data | Recommended | Recommended | |
| Customized Files | Configuration or other files that have been customized | Important | Important | Important |
| Windows Registry | Settings for the Harvesters | | Important (Windows) | |

The following list describes the databases and their locations:

- reporter database: Back up the previous 24 hours of Enterprise Overview data, NFA console configuration settings, and synchronization information.

  Path: <install_path>\MySql51\data\reporter directory

- harvester database: Back up the Harvester configuration data.

  Path: <install_path>\MySql51\data\harvester directory

- Nqrptr database: (Recommended) Back up the historical (15-minute) data that is stored for the reporting routers and interfaces.

  Path: <install_path>\MySql51\data\nqrptr directory

- Customized configuration files: Back up any customized configuration files--files that you customized or that were customized by CA Support. In addition, back up any customizations that you made to the website or reports.

  The CA Network Flow Analysis configuration files typically have a .config, conf., or .ini extension and are located in the product installation path. Other customizations may include .css files and report logos.

- Windows Registry: Back up the Windows Registry on Harvester servers. Harvester Registry settings are converted to MySQL database settings during the upgrade.

  Back up the Registry as a .reg file by selecting File, Export in the Registry Editor window. For more information about the new location of Harvester settings, see the Release Notes topic "Relocation of Harvester Settings."

**Important:**

- Make the backups run concurrently. If you restore data from backups that have different timestamps, problems can result. Ensure that your backed-up data files are timestamped with the same hour.
- Store backups to a remote location to guard against the possibility of a hardware or OS failure on the main server. For example, back up the databases to an administrative share or mapped network drive.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Connect to the server:
   a. Open a Remote Desktop session.
   b. Initiate a Terminal Services or VNC session to the installation server.
3. Copy each of the following directories or files to a remote location:
   - Reporter database: Copy the following directory from the standalone server or the NFA console server of a distributed deployment:
     <install_path>\MySql51\data\reporter
   - Nqrptr database: Copy the following directory from the standalone server or the DSA server of a distributed deployment:
     <install_path>\MySql51\data\nqrptr
   - Customized configuration files: Back up any customized configuration files from the CA Network Flow Analysis installation path on any server. In addition, back up files that have been changed to customize reports, such as .css files and report logos.
4. Restart the services (see page 47).

## Back Up 9.1.00 and 9.1.1 Databases

Before you upgrade a CA Network Flow Analysis 9.1.00 or 9.1.1 deployment, back up the databases and files that are listed in the following table.

**Important:**

- Make the backups run concurrently. If you restore data from backups that have different timestamps, problems can result. Ensure that your backed-up data files are timestamped with the same hour.
- Store backups to a remote location to guard against the possibility of a hardware or OS failure on the main server. For example, back up the databases to an administrative share or mapped network drive.

| Database | Description | Standalone Server | Harvester Servers (Distributed) | NFA Console Server (Distributed) |
|---|---|---|---|---|
| reporter | Enterprise Overview data and NFA console configuration data | Important | | Important |
| harvester | Harvester configuration data | Important | Important | |
| poller | Poller configuration data | Important | Important | |
| ReaperArchive15 | Historical (15-minute) data | Recommended | Recommended | |
| Customized Files | Configuration or other files that have been customized | Important | Important | Important |
| Customized data_retention | Settings to regulate data retention | Important if customized | Important if customized | |
| ReaperArchive | Realtime (1-minute) data | Optional, rarely backed up | Optional, rarely backed up | |
| Windows Registry | Settings for the Windows Harvesters | | Important (Windows Harvesters) | |

The following list describes the databases and their locations:

- reporter database: Back up the previous 24 hours of Enterprise Overview data, NFA console configuration settings, and synchronization information.

  Path: <install_path>\MySql51\data\reporter directory

- harvester database: Back up the Harvester configuration data.

  Path: <install_path>\MySql51\data\harvester directory

- poller database: Back up the Poller configuration data. The poller and harvester configuration data are essential to perform the relational mapping that provides access to 15-minute data. The poller configuration data provides information about devices and interfaces to enable polling, such as persistent IDs for interfaces.

  Path: <install_path>\MySql51\data\poller directory

- ReaperArchive15 database: Optionally, back up the historical (15-minute) data that is stored for the reporting routers and interfaces. This backup is optional, but many administrators do back up the 15-minute data.

  Path: <install_path>\Netflow\datafiles\ReaperArchive15 directory

- Customized configuration files: Back up any customized configuration files--files that you customized or that were customized by CA Support. In addition, back up any customizations that you made to the website or reports.

  The CA Network Flow Analysis configuration files typically have a .config, conf., or .ini extension and are located in the product installation path. Other customizations may include .css files and report logos.

- ReaperArchive database: (Recommended) Back up the historical (15-minute) data.

  Path: <install_path>\Netflow\datafiles\ReaperArchive directory

- Customized data_retention database: If you customized any data retention settings, back up the data retention configuration data. It is unusual to customize data retention settings except with the assistance of CA Support. Changes to data retention settings can cause problems from rising demands on drive space.

  Path: <install_path>\MySql51\data\data_retention directory

- Windows Registry: Back up the Windows Registry on Windows Harvester servers. Harvester Registry settings are converted to MySQL database settings during the upgrade.

  Back up the Registry as a .reg file by selecting File, Export in the Registry Editor window. For more information about the new location of Harvester settings, see the Release Notes topic "Relocation of Harvester Settings."

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Connect to the server:
   a. Open a Remote Desktop session.
   b. Initiate a Terminal Services or VNC session to the installation server.
3. Copy each of the target directories or files to a remote location.
4. Restart the services (see page 47).

# Chapter 6: Install the Software

This section contains the following topics:



## Upgrade a Standalone Server

A *standalone deployment* consists of a single server that hosts all of the components: the Harvester and the NFA console. Complete the steps in this topic to upgrade the Harvester and NFA console on a single Windows server or virtual machine.

**Notes:**

- A standalone upgraded deployment of CA Network Flow Analysis 9.1.3 uses a two-tier architecture, even if you previously had a standalone deployment with three-tier architecture.
- If you interrupt and restart the upgrade, the upgrade resumes from your most recently saved change.

**Before You Begin:** Verify that the server is upgrade-ready as described in Verify Preparation of the Windows Servers (see page 21).

**Follow these steps to complete the Harvester phase of the upgrade:**

1. Run the Console tool:
   a. Log in to the standalone server as a user with administrator privileges for the system and for CA Network Flow Analysis.
   b. Verify that the consoletool-exe.jar file is on the server--for example, on the Desktop. If you do not have this file, download it. (see page 14)

      The Console tool prepares the system for the upgrade (see page 100).

c. Double-click the consoletool-exe.jar file in Windows Explorer or enter the following string at a command prompt:

```
java –jar consoletool-exe.jar
```

To launch the Console tool by double-clicking the file, Windows Explorer must have the correct association for .jar files.

The ConsoleInfoToPollerTool<yyyy-mm--dd>.log file opens when the Console tool completes--whether the tool completes successfully or fails. The log is saved in the <install_path>\Reporter\Logs\ directory.

The Console tool cannot complete successfully if the system has undeployed interface aggregations or unscheduled merge or delete interface tasks. If the tool does not complete successfully, note the error messages in the log file and contact CA Support.

2. Stop the pump service:
   a. Click Start, Programs, Administrative Tools, Services.
   b. Right-click the NetQoS Reporter/Analyzer Pump service.
   c. Select Stop in the right-click menu.

      The pump service stops.
3. Start the Harvester phase of the upgrade: Double-click the NFHarvesterSetup9.1.3.exe file. If you do not have this file, download it to the server as described in Prerequisites (see page 14).

   A check verifies that the server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 102). You cannot launch the installation or upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.
4. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.
5. Click Next in the Welcome screen.

   The CA NFA Harvester License Agreement screen opens.
6. Review and accept the license agreement:
   a. Read the license agreement and scroll down.
   b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.
   c. Click Next.

Prerequisite tests are run to identify problems on the server. If a problem is found, an error message opens. A critical problem causes the program to exit. A Pre-requisite Check Warning message or other warning message opens for non-critical problems, which gives you the option to make corrections now or after the installation or upgrade is complete.

7. Review the test results in the Pre-requisite Check Warning message, if it opens:
   a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting (see page 99) section.
   b. Click OK to close the message.

      Your system is tested to determine whether the installed version of CA Network Flow Analysis is supported for upgrade. If a supported version is located, the Upgrading Existing Installation message opens.

      Once the server passes the required checks and you close any warning messages that appear, the Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.
8. Verify that the specified installation directory is correct, then click Next.

   **Important:** If you do not use the original installation path, the upgraded software will not run properly.

   If the program does not find certain expected directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

   The Pre-Installation Summary screen opens.
9. Review the pre-installation information, then click Install.

   The Installing Harvester screen opens, which shows the progress. When the upgrade is complete, the Install Complete screen opens and reports any errors that occurred.
10. (Optional) If errors occurred during the upgrade, see the following logs for details:
    - General installation log: <install_path>\Harvester_Install_<timestamp>.log (where <timestamp> is the time that the log was created)
    - Upgrade migration log: <install_path>\migrator.log
11. Click Done in the Install Complete screen.

    The Harvester upgrade program closes.

**Follow these steps to complete the NFA console phase of the upgrade:**

1. Start the NFA console upgrade software: Double-click the RAConsoleSetup9.1.3.exe file in Windows Explorer. If you do not have this file, download it to the server as described in Prerequisites (see page 14).

   A check verifies whether a supported version of the Java Runtime Engine (JRE) is installed. If the check fails, an error message opens (see page 102). You cannot launch the upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.

2. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.

3. Click Next in the Welcome screen.

   The NFA Console License Agreement screen opens.

4. Review and accept the license agreements:

   a. Read the NFA console license agreement and scroll down.

   b. If you want to continue under the terms of the NFA console license agreement, click the option to accept it This option is activated when you scroll to the bottom.

   c. Click Next.

      The Third-Party License Agreement screen opens.

   d. Read the third-party license agreement and scroll down.

   e. If you want to continue under the terms of the third-party license agreement, click the option to accept it. This option is activated when you scroll to the bottom.

   f. Click Next.

      Prerequisite tests are run on the server. If an error message opens that requires attention, see Troubleshooting (see page 99).

5. Review the test results in the Pre-requisite Check Warning message, if it opens:

   a. Correct any noncritical problems now or wait until the upgrade program finishes.

   b. Click OK to close the message.

      A test verifies that the installed version of CA Network Flow Analysis is supported for upgrade. The Singlebox Confirmation message opens when the verification is complete. This message asks you to confirm that you want a standalone deployment of CA Network Flow Analysis.

6. Review the Singlebox Confirmation information and click OK.

   The Pre-Installation Summary screen opens after a moment.

7. Review the pre-installation information, then click Install.

   The Installing NFA screen opens. Progress is shown in the status bar and messages. When the NFA console upgrade is complete, the Install Complete screen opens.

8. Exit from the upgrade program:

   a. Select one of the restart options:

      - Yes, restart my system: Restart the system as soon as you click Done.
      - No, I will restart my system myself: Defer the restart to be performed manually.

   b. Click Done.

      The upgrade program closes after a moment. If you selected the option to restart now, the system restarts and the upgrade is finalized.

      If you upgraded from ReporterAnalyzer 9.0.1, migration of DSA database table data begins as soon as the CA NFA DSALoader service restarts. If you have many agents and an extensive amount of stored data, migration may continue for some time. When migration is complete, the CA NFA DSALoader service stops itself and does not restart. The service state change is recorded in the following log: \Netflow\Logs\dsaLoaderErrors-<yyyy-mm-dd>.log. Reports have limited access to historical (15-minute) data until the migration is complete.

**Note:** The revision history shows that the software is upgraded to the correct version. To display the revision history, complete the following substeps:

1. Start MySQL by entering the following command in a Command Prompt window:
   mysql
2. Display the revision history by entering the following command:
   select * from revision_history

**Next:** Complete the post-upgrade tasks (see page 75).

# Upgrade a Distributed Deployment

In a distributed deployment, CA Network Flow Analysis components are distributed among multiple servers. The topics in this section describe how to upgrade each component server.

To upgrade a two-tier distributed deployment, complete the following procedures:

- Upgrade the Harvester on a Windows Server (see page 60), or
- Upgrade the Harvester on a Linux Server (see page 63)
- Upgrade the Console (see page 70)

To upgrade a three-tier distributed deployment, complete the following procedures:

- Upgrade the Harvester on a Windows Server (see page 60)
- Upgrade the DSA Server (see page 67)
- Upgrade the Console (see page 70)

**Notes:**

- The steps in these topics are written for the recommended upgrade order: Harvester upgrades, DSA upgrades (if any), then NFA console upgrade.
- If you interrupt and restart the upgrade, the upgrade resumes from your most recently saved change.

## Upgrade the Harvester on a Windows Server

In a distributed deployment, each Harvester is installed on a separate server. To upgrade a Harvester on a dedicated Windows server or virtual machine, complete the steps in this topic. These steps apply to a two-tier or three-tier distributed deployment.

**Before You Begin:** Verify that the server is upgrade-ready as described in Verify Preparation of the Windows Servers (see page 21).

**Follow these steps to prepare the NFA console server for the Harvester upgrade:**

1. Run the Console tool:
   a. Log in to the NFA console server as a user with administrator privileges for the system and for CA Network Flow Analysis.
   b. Verify that the consoletool-exe.jar file is on the NFA console server in a location such as the Desktop. If you do not have this file, download it. (see page 14)

      The Console tool prepares the system for the upgrade (see page 100).

c. Double-click the consoletool-exe.jar file in Windows Explorer or enter the following string at a command prompt:

```
java –jar consoletool-exe.jar
```

To launch the Console tool by double-clicking the file, Windows Explorer must have the correct association for .jar files.

The ConsoleInfoToPollerTool<yyyy-mm--dd>.log file opens when the Console tool completes--whether the tool completes successfully or fails. The log is saved in the <install_path>\Reporter\Logs\ directory.

The Console tool cannot complete successfully if the system has undeployed interface aggregations or unscheduled merge or delete interface tasks. If the tool does not complete successfully, note the error messages in the log file and contact CA Support.

2. Stop the pump service on the NFA console server:
   a. Click Start, Programs, Administrative Tools, Services.
   b. Right-click the NetQoS Reporter/Analyzer Pump service.
   c. Select Stop in the right-click menu.

      The service stops.

**Follow these steps to upgrade the Harvester:**

1. Start the upgrade: Double-click the NFHarvesterSetup9.1.3.exe file in Windows Explorer on the Harvester server. If you do not have this file, download it. (see page 14)

   A check verifies that the server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 102). You cannot launch the installation or upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.

2. Verify that the appropriate language is selected, then click OK.

   A check verifies whether the installed version of CA Network Flow Analysis is supported for upgrade. If a supported version is found, the Prior Installation Detected message opens.

3. Review the Prior Installation Detected message and click OK. If the installed CA Network Flow Analysis version is not supported for upgrade, upgrade to a supported version (see page 13).

   The Welcome screen opens.

4. Click Next in the Welcome screen.

   A check verifies that the Console tool completed successfully on the NFA console server. If the tool did not run successfully, an error message opens and the upgrade stops.

   If the server passes the check, the CA NFA Harvester License Agreement screen opens.

5. Review and accept the license agreement:

   a. Read the license agreement and scroll down.

   b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.

   c. Click Next.

      Prerequisite tests are run to identify problems on the server. If a problem is found, an error message opens. A critical problem causes the upgrade program to exit. If the problem is not critical, the Pre-requisite Check Warning message or other warning message opens, which gives you the option to make corrections now or after the upgrade is complete.

      Once the server passes the required checks and you close any noncritical messages that appear, the Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.

6. If the Pre-requisite Check Warning message opens, review the test results:

   a. Correct the problems now or wait until the upgrade program finishes. For more information about the warnings, see the Troubleshooting (see page 99)section.

   b. Click OK to close the message.

      Once the server passes the required checks successfully and you dismiss any warnings that appear, the Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.

7. Verify that the specified installation directory is correct, then click Next.

   **Important:** If you do not use the original installation path, the upgraded software will not run properly.

   If the program does not find certain expected directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

   The Pre-Installation Summary screen opens.

8. Review the pre-installation information, then click Install.

   The Installing Harvester screen opens, which shows the upgrade progress. When the upgrade is complete, the Install Complete screen opens and reports any errors that occurred.

9. (Optional) If errors occurred during the upgrade, see the following logs for details:
   - General installation log: <install_path>\Harvester_Install_<timestamp>.log.
   - Upgrade migration log: <install_path>\migrator.log
10. Exit from the upgrade program:
    a. Select one of the restart options:
       - Yes, restart my system: Restart the system as soon as you click Done.
       - No, I will restart my system myself: Defer the restart to be performed manually.
    b. Click Done.

       The upgrade program closes after a moment. If you selected the option to restart now, the system restarts and the upgrade is finalized.
11. (Optional) Verify that the following conditions are met:
    - Harvester services are running.
    - Harvester is receiving data.
    - The revision history shows that the component is upgraded to the correct version. To display the revision history, complete the following substeps:
      a. Start MySQL by entering the following command in a Command Prompt window: mysql
      b. Display the revision history by entering the following command: select * from revision_history

**Next:**

- To upgrade another Harvester, repeat these steps on the additional Harvester server.
- To continue upgrading a two-tier deployment, Upgrade the Console Server (see page 70).
- To continue upgrading a three-tier deployment, Upgrade the DSA Server (see page 67).

## Upgrade the Harvester on a Linux Server

A two-tier distributed deployment of CA Network Flow Analysis may include one or more Linux Harvester servers. To upgrade the Harvester software on a dedicated Linux server or virtual machine, complete the steps in this topic.

**Before You Begin:** Verify that the server is upgrade-ready as described in Verify Preparation of the Linux Servers (see page 41).

**Follow these steps to prepare the NFA console server for the Harvester upgrade:**

1. Run the Console tool:

   a. Log in to the NFA console server as a user with administrator privileges for the system and for CA Network Flow Analysis.

   b. Verify that the consoletool-exe.jar file is on the NFA console server in a location such as the Desktop. If you do not have this file, download it. (see page 14)

      The Console tool prepares the system for the upgrade (see page 100).

   c. Enter the following string at a command prompt:

      ```
      java –jar consoletool-exe.jar
      ```

      The ConsoleInfoToPollerTool<yyyy-mm--dd>.log file opens when the Console tool completes--whether the tool completes successfully or fails. The log is saved in the <install_path>\Reporter\Logs\ directory.

      The Console tool cannot complete successfully if the system has undeployed interface aggregations or unscheduled merge or delete interface tasks. If the tool does not complete successfully, note the error messages in the log file and contact CA Support.

2. Stop the pump service on the NFA console server:

   a. Click Start, Programs, Administrative Tools, Services.

   b. Right-click the NetQoS Reporter/Analyzer Pump service.

   c. Select Stop in the right-click menu.

      The pump service stops.

**Follow these steps to upgrade the Harvester:**

1. Log in to the target system as root.

   You can install the software locally or remotely--for example, by using ssh when you are logged in with root privileges.

   **Note:** If you do not have root access, use an account with sudo privileges.

2. Open a command prompt window.

3. Run the following command to change the ulimit for the open files limit:
   `ulimit -n ulimit_number`

   **Example:**
   `ulimit -n 65536`

4. Prepare the installation/upgrade file for execution:

   a. Log in to the Harvester server as root.

      You can install or upgrade the software locally or remotely--for example, by using ssh when you are logged in with root privileges. If you do not have root access, use an account with sudo privileges.

b. Execute the chmod command on the file in a terminal window:
`chmod u+x NFHarvesterSetup9.1.3.bin`

c. (Optional) Execute the list command to verify that the file is executable:
`ls -al`

The file permission settings are displayed.

5. Run the installation or upgrade software:
`./NFHarvesterSetup9.1.3.bin`

A check verifies that the server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 102). You cannot launch the installation or upgrade program until this problem is corrected.

If the server passes the Java prerequisite check, the program starts and the language selection screen opens.

6. Verify that the appropriate language is selected, then click OK.

A check determines whether the installed version of CA Network Flow Analysis is supported for upgrade. If a supported version is located, the Prior Installation Detected message opens.

7. Review the Prior Installation Detected message and click OK to close it. If a supported software version is not installed, upgrade to a supported version (see page 13).

The Welcome screen opens.

8. Click Next in the Welcome screen.

A check verifies that the Console tool completed successfully on the NFA console server. If the tool did not run successfully, an error message opens and the upgrade stops.

If the server passes the check, the License Agreement screen opens.

9. Review and accept the license agreement:

a. Read the license agreement and scroll down.

b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.

Prerequisite tests are run to identify problems on the server. If a problem is found, an error message opens. A critical problem causes the upgrade program to exit. If the problem is not critical, the Pre-requisite Check Warning message or other warning message opens, which gives you the option to make corrections now or after the upgrade is complete.

10. If the Pre-requisite Check Warning message opens, review the test results:

a. Correct the problems now or wait until the upgrade program finishes. For more information about the warnings, see the Troubleshooting (see page 99)section.

b. Click OK to close the message.

Once the server passes the required checks successfully and you dismiss any warnings that appear, the Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.

11. Verify that the specified installation directory is correct, then click Next.

**Important:** If you do not use the original installation path, the upgraded software will not run properly.

If the program does not find certain expected directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

The Pre-Installation Summary screen opens.

12. Review the pre-installation information, then click Install.

The Installing Harvester screen opens, which shows the upgrade progress. When the upgrade is complete, the Install Complete screen opens and reports any errors that occurred.

13. (Optional) Review errors that occurred by checking the installation log (Harvester_Install_<timestamp>.log in the <install_path> directory).

14. Click Done.

The upgrade program closes. The Harvester is upgraded and the CA Network Flow Analysis services are started.

15. (Optional) Verify that the following conditions are met:

- (Two-tier architecture deployment) Harvester services are running.
- Harvester is receiving data.

- The revision history shows that the component is upgraded to the correct version. To display the revision history, complete the following substeps:
  a. Start MySQL by entering the following command in a Command Prompt window: mysql
  b. Display the revision history by entering the following command: select * from revision_history

**Next:**

- To upgrade another Harvester, repeat these steps on the additional Harvester server.
- To continue upgrading a two-tier deployment, Upgrade the Console Server (see page 70).
- To continue upgrading a three-tier deployment, Upgrade the DSA Server (see page 67).

## Upgrade the DSA in a Three-Tier Distributed Deployment

In a three-tier distributed deployment, each DSA is installed on a separate server. To upgrade a DSA on a dedicated Windows server or virtual machine, complete the steps in this topic.

**Before You Begin:** Verify that the installation server meets the following requirements:

- The server is upgrade-ready as described in Verify Preparation of the Windows Servers (see page 21).
- The Harvester servers have been upgraded (see page 60).
- The Console tool has been run on the NFA console server, as described at the beginning of Upgrade the Harvester. (see page 60)

**Note:** If you have a Linux DSA, contact your CA Support Availability Manager or Sales Account team to inquire about obtaining a Windows-based DSA.

**Follow these steps:**

1. Verify that processing is complete for the collected DSA data:
   a. Log in to the NFA console server with an account that has administrator privileges for CA Network Flow Analysis.
   b. Locate the following directory on the NFA console server:
   <install_path>\Reporter\datashare\data\<DSA_server_IP_address>
   c. Verify that the directory does not contain any .csv files. If .csv files are present, keep checking until the files are gone. The files are processed and gone within 15 minutes.
2. Start the upgrade: Double-click the DSASetup9.1.3.exe file in Windows Explorer.

   A check verifies that the server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 102). You cannot launch the installation or upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.
3. Verify that the appropriate language is selected, then click OK.

   The License Agreement screen opens.
4. Review and accept the license agreement:
   a. Read the license agreement and scroll down.
   b. If you want to continue under the terms of the license agreement, click the option to accept it. This option is activated when you scroll to the bottom.
   c. Click Next.

      Prerequisite tests are run to identify problems on the server. If a problem is found, an error message opens. A critical problem causes the program to exit. A Pre-requisite Check Warning message or other warning message opens for non-critical problems, which gives you the option to make corrections now or after the installation or upgrade is complete.
5. Review the test results in the Pre-requisite Check Warning message, if it opens:
   a. Correct problems now or wait until the program finishes. For more information about the warnings, see the Troubleshooting (see page 99) section.
   b. Click OK to close the message.

      The upgrade can proceed only if the previous software version is supported for the upgrade. If you do not have a supported software version installed, upgrade to a supported version (see page 13) before you proceed.

      Once the server passes the required checks and you close any warning messages that appear, the Choose Install Folder screen opens. This screen displays the original root installation path as the default setting.

6. Proceed through the options to verify the installation directories:
   a. Click Next in the Choose Install Folder screen.

      **Important:** If you do not use the original installation path, the upgraded software will not run properly.

      If the program does not find certain expected directories in the installation path, an error message opens and the upgrade stops. This problem does not occur when the previous software installation is fully functional.

      The Select a Location for the MySQL Data Directory screen opens after a moment. This screen shows the original installation path for the MySQL data directory.

      The Folder Selected Is Not Empty message also opens, which asks you to verify that you have backed up the directory contents.

   b. Click Next in the Select a Location for the MySQL Data Directory screen.

      **Important:** If you do not use the original installation path, the upgraded software will not run properly.

      The Select a Location for the MySQL Temp Directory screen opens, which shows the original installation path for the MySQL tmp directory.

   c. Click OK to close the message.

   d. Click Next in the Select a Location for the MySQL Temp Directory screen.

      **Important:** If you do not use the original installation path, the upgraded software will not run properly.

      MySQL51 is configured, then the Pre-Installation Summary screen opens.

7. Review the pre-installation information, then click Install.

   The Installing DSA screen opens, which shows the progress of the upgrade. When the upgrade is complete, the Install Complete screen opens. This screen tells you whether any errors occurred during the upgrade.

8. Click Done.

   The upgrade program closes. The DSA is upgraded and the DSA services are restarted.

9. (Optional) Verify that the following conditions are met:
   - DSA services are running.
   - The DSA is receiving data.

- The revision history shows that the component is upgraded to the correct version. To display the revision history, complete the following substeps:
  a. Start MySQL by entering the following command in a Command Prompt window: mysql
  b. Display the revision history by entering the following command: select * from revision_history

10. (Optional) Check the DSA_Install_<timestamp> log periodically. This log is located at the install path root level--for example, in the \\CA\NFA directory. Use the log to monitor the migration of the DSA database tables to the new format.

    The migration of DSA database table data begins as soon as the CA NFA DSALoader service restarts. The DSA_Install log lists the tables as they are migrated. Nine tables are migrated for each agent or interface. If you have many agents and an extensive amount of stored data, migration may continue for some time.

**Next:**

- To upgrade an additional DSA on another server, repeat these steps.
- To upgrade the console server (see page 70), go to the next topic.

## Upgrade the NFA Console

Distributed deployments use separate servers for the NFA console, Harvesters, and any DSAs in the deployment. Complete the steps in this topic to upgrade the NFA console on a dedicated Windows server or virtual machine.

**Before You Begin:** Verify that the server meets the following requirements:

- The server is upgrade-ready as described in Verify Preparation of the Windows Servers (see page 21).
- The Harvester servers have been upgraded (see page 60).
- If you have a three-tier architecture deployment, the DSA servers have been upgraded (see page 67).
- If you are upgrading from CA NetQoS ReporterAnalyzer 9.0.1, the NetQoS Reporter/Analyzer Pump service on the NFA console server remains stopped after the Harvester upgrades.

**Follow these steps:**

1. Log in to the NFA console server as a user who has administrator privileges for the system and for CA Network Flow Analysis.

2. (Three-tier architecture only) Verify that the DSAs have picked up all the 15-minute data from the NFA console server:

   a. Locate the following directory on the NFA console server: <install_path>\reporter\datashare\data\<DSA_server_IP_address>

   b. Verify that the directory does not contain .csv files. If .csv files are present, wait until the files are gone. Once you stop the pump service, the .csv files should be gone within 15 minutes.

3. Start the upgrade: Double-click the RAConsoleSetup9.1.3.exe file in Windows Explorer on the NFA console server.

   A check verifies that the server has a supported version of the Java Runtime Engine (JRE) installed. If the check fails, an error message opens (see page 102). You cannot launch the installation or upgrade program until this problem is corrected.

   If the server passes the Java prerequisite check, the program starts and the language selection screen opens.

4. Verify that the appropriate language is selected, then click OK.

   The Welcome screen opens.

5. Click Next in the Welcome screen.

   The License Agreement screen opens.

6. Review and accept the license agreements:

   a. Read the NFA console license agreement and scroll down.

   b. If you want to continue under the terms of the NFA console license agreement, click the option to accept it This option is activated when you scroll to the bottom.

   c. Click Next.

      The Third-Party License Agreement screen opens.

   d. Read the third-party license agreement and scroll down.

   e. If you want to continue under the terms of the third-party license agreement, click the option to accept it. This option is activated when you scroll to the bottom.

   f. Click Next.

      Prerequisite tests are run on the server, as described in Troubleshooting (see page 99). If the server fails any noncritical tests, the Pre-requisite Check Warning message opens. If the server fails the test to verify the presence of the Service Control command, a separate error message opens.

7. If the Pre-requisite Check Warning message opens, review the test results:

   a. Correct the problems now or wait until the upgrade program finishes. For more information about the warnings, see the Troubleshooting (see page 99)section.

b. Click OK to close the message.

A test verifies that the installed version of CA Network Flow Analysis is supported for upgrade. The Upgrading Existing Installation message opens when the verification is complete.

8. Review the Upgrading Existing Installation information.

a. Verify that the version information is correct in the Upgrading Existing Installation screen that opens. The message reports the existing CA Network Flow Analysis version and the post-upgrade version.

b. Click OK to close the message.

The Upgrading Existing Installation message reopens and reports the root installation path. The upgrade program always uses the original path. The default path is C:\CA\NFA.

c. Review the path information in the new Upgrading Existing Installation message.

d. Click OK to close the message.

The Choose Install Folder screen opens.

9. (Optional) Click Choose to change the program installation location when prompted or enter a new path manually.

The default location is C:\CA\NFA. We recommend that you install CA Network Flow Analysis components on a nonsystem drive that you have set up for CA Network Flow Analysis. Use the same installation path for the Harvester and console servers.

The Pre-Installation Summary screen opens after a moment.

10. Review the pre-installation information, then click Install.

The Installing NFA screen opens. Progress is shown in the status bar and messages. When the NFA console upgrade is complete, the Install Complete screen opens and reports any errors.

11. (Optional) If errors occurred during the upgrade, see the installation log: <install_path>\NFA_Install_<timestamp>.log.

12. Exit from the upgrade program:

a. Select one of the restart options:

- Yes, restart my system: Restart the system as soon as you click Done.
- No, I will restart my system myself: Defer the restart to be performed manually.

b. Click Done.

The upgrade program closes after a moment. If you selected the option to restart now, the system restarts and the upgrade is finalized.

If you upgraded from ReporterAnalyzer 9.0.1, DSA database migration may continue for some time. Reports will have limited access to historical (15-minute) data until the migration is complete.

**Note:** The revision history shows that the software is upgraded to the correct version. To display the revision history, complete the following substeps:

1. Start MySQL by entering the following command in a Command Prompt window:
   mysql
2. Display the revision history by entering the following command:
   select * from revision_history

**Next:** Complete the post-upgrade tasks (see page 75).

# Chapter 7: Post-Upgrade Tasks

Complete the following post-installation tasks:

- If you are using CA Network Flow Analysis with CA NetQoS Performance Center, make sure you have the supported version in your environment. (see page 13)
- Configure SNMP on any Linux Harvesters that are in your deployment. (see page 80)
- Verify that your trap receivers are configured.as described in Reconfigure Trap Receivers (see page 86).
- Exclude the following directories from real-time scans: C:\Windows\Temp and <install_path> and all its subdirectories. Real-time scans of these directories can corrupt the database.
- Do not implement drive space compression. Drive space compression can cause database losses and degraded system performance.

<table>
<tr><th>Standalone Server</th><th>Distributed NFA Console Server</th><th>Distributed Harvester Server (Windows)</th><th>Distributed 3-Tier DSA Server</th></tr>
<tr><td colspan="4">■ Synchronize system time between all servers (Windows Server 2008 (see page 81) or 2003 (see page 82)).</td></tr>
<tr><td colspan="2">■ (Recommended) Update the list of trusted internet sites. (see page 83) *</td><td colspan="2"></td></tr>
<tr><td>■ (Recommended) Modify router ACLs. (see page 84) **</td><td></td><td>■ (Recommended) Modify router ACLs. (see page 84) **</td><td></td></tr>
<tr><td colspan="2">■ (Recommended, Windows Server 2008 only) Disable UAC. (see page 85)</td><td colspan="2"></td></tr>
<tr><td colspan="2">■ (Recommended) Configure Web content expiration [Windows Server 2008 (see page 32) or 2003 (see page 89)].</td><td colspan="2"></td></tr>
<tr><td colspan="4">■ (Recommended) Add a key to prevent SNMP false positives. (see page 90)</td></tr>
</table>

| Standalone Server | Distributed NFA Console Server | Distributed Harvester Server (Windows) | Distributed 3-Tier DSA Server |
|---|---|---|---|
| ■ (Optional) Configure the Recycle Bin. (see page 91) | | | |
| ■ (Optional) Disable unneeded services [Windows Server 2008 (see page 92) or 2003 (see page 94)]. | | | |

* In addition to the standalone server or NFA console server, verify that this task has been completed for the browsers on the systems that access the NFA console.

** In a distributed deployment, verify that the router access control lists (ACLs) are configured to enable the Harvesters to perform SNMP polling.

This section contains the following topics:

# Upgrade or Register with CA Performance Center

The NFA console or standalone server must be registered as a data source with a supported version of CA Performance Center or CA NetQoS Performance Center:

- Upgrade from CA NetQoS ReporterAnalyzer 9.0.1: Operate with CA Performance Center 2.2.x, CA Performance Center 2.3.x, or CA NetQoS Performance Center 6.1.194.
- Upgrade from CA NetQoS ReporterAnalyzer 9.1.00 or later: Operate with CA Performance Center 2.2.x or 2.3.x.

The registration task depends on your upgrade type:

- If you previously unregistered from CA NetQoS Performance Center or CA Performance Center and you have completed the CA Network Flow Analysis upgrade, follow the steps in this topic to register as a data source for CA Performance Center 2.2.x or 2.3.x.
- If you have not unregistered and you have CA Performance Center 2.1.x currently installed, perform the upgrade to CA Performance Center version 2.2.x or the incremental upgrades to version 2.3.x now. For instructions, see the *CA Performance Center Installation Guide*.
- If you upgraded from CA NetQoS ReporterAnalyzer 9.0.1 and you want to keep using CA NetQoS Performance Center 6.1.194, you should already be registered. In this case, skip this step.

**Follow these steps:**

1. Log in to the CA Performance Center Console as a user with the Administrator role.
2. Navigate to the Manage Data Sources page.

   The Manage Data Sources page displays the current list of registered data sources.
3. Click Add.

   The Add Data Source dialog opens.
4. Select CA Network Flow Analysis from the Source Type list.

   **Note**: All CA products that can be registered as CA Performance Center data sources are shown in the Source Type list. The list is not filtered to show installed products.
5. Select the data source status. Select Disabled if you want to delay polling of this data source while still registering it.

   No data from this data source is reported until you edit the data source to select the Enabled status. Views from this data source display a message stating, "No data to display".
6. Enter the Host Name: Use the IP address or DNS hostname of the NFA console server.

7. Enter the port to use when contacting the data source. The port that you enter depends on the protocol you select.

   For more information, see the *CA Single Sign-On User Guide*.

8. Select the protocol to use to contact the data source. Select **https** if your network is using SSL for communications. Verify that you have configured the system correctly before you select the **https** option.

   **Note**: SSL can be used for communications between CA Performance Center and the data source products. For more information, see the *CA Single Sign-On User Guide.*

9. (Optional) Enter a Display Name for the data source.

   By default, the data source type and the hostname are combined to create the display name. You can supply another name here. For example, instead of NetworkFlowAnalysis@xxx.x.x.xx, you can name the data source NetworkFlowAnalysis_NewYork.

10. Click Save to register the data source.

    The Data Source List shows the CA Network Flow Analysis deployment that you registered.

11. Review the results in the CA Performance Center Console and make any adjustments that are needed. Review the list of potential changes that are described in the topic about unregistering (see page 37). For example, revise the following elements as needed:

    - Tenants and domains: Recreate any custom tenants and domains that are missing. Reassign groups, user accounts, devices, and interfaces to the custom tenants and domains. Restore the protocol names, ToS labels, AS names, and IP addresses that were in custom domains.
    - Users: Check or spot-check the user accounts, their settings, and their assigned groups and domains.
    - Groups:
      - Relocate groups as needed.
      - Delete any duplicate groups.
      - Restore any deleted groups, including any dynamic groups such as cross-product groups.

- SNMP profiles: Check the SNMP profiles and any domain assignments that they had before the unregister process.

- LDAP and other Single Sign-On customizations: Check.

  **Note:** If you upgrade from CA NetQoS ReporterAnalyzer 9.0.1, you also will change to a new SSO version. Update any previous SSO LDAP configuration and check other SSO customizations. Options from the previous SSO version may not match the current options or may not comprise a full set of the current options. For information about configuring SSO, see the *Single Sign-On User Guide*.

12. Check the effects of your revisions in the NFA console. For example, review the following locations:

    - Active Interfaces page:

      a. Select Administration, Interfaces: Physical & Virtual.

      b. Verify that expected routers and interfaces are shown.

      c. Check the domain assignments for interfaces: Select an interface, click Edit, and verify that the expected tenant / domain setting is shown in the Edit Interface dialog.

      d. Verify that the Domain list contains the expected domains.

    - Available Interfaces page: Select Administration, System: Enable Interfaces. Verify that the expected routers and interfaces are shown as enabled.

    - Interface Index Group tab: Select Interfaces, Group tab. Verify that the group tree in the left pane has the expected contents and structure.

      If an HTTP Request Error opens when you attempt to display the Group tab, clear your browser cache. The error may indicate that you browser is attempting to reload an outdated page.

    - Harvester page: Select Administration, System: Harvester. Verify that the Harvester tenant / domain assignments are correct.

    - Domain-specific ToS labels: Select Administration, Groups: ToS Groups. Verify that the expected ToS labels are shown for each ToS group with domain-specific ToS labels.

    - Domain-specific protocol names: Select Administration, Groups: Protocol Groups. Verify that the expected protocol names are shown for each protocol group when you select the group and click List.

    - Domain-specific AS names: Select Administration, Define an Application: AS Names. Verify that the expected AS names are shown for each domain that you select.

    - Enterprise Overview page, Interfaces pages, and report pages: Verify that the expected contents are visible to users who have varying types of access.

# Configure SNMP on Linux Servers

To configure a Linux server for a Harvester, complete the following tasks:

- Set up the Net-SNMP configuration file.
- Configure SNMP to start automatically on boot.
- Start the snmpd service.

**Follow these steps:**

1. Log in as root and open a shell prompt.
2. Highly Recommended: Use the following steps to set up the Net-SNMP configuration file. This configuration file is needed for Watchdog SNMP polling.

   **Note:** If you have a custom (non-default) snmp configuration file at /etc/snmp/snmp.conf, you may want to skip this step and update your existing configuration file instead. In this case, consult with an administrator to update the required settings to match the settings in the example configuration file. For example, make sure the rocommunity value is set as shown in the example configuration file.

   If you use a custom community name as the rocommunity value, use the same community name throughout the CA Network Flow Analysis deployment:

   - The snmpd.conf file on each Linux Harvester server
   - SNMP service on each Windows server
   - Watchdog Settings page of the NFA console

   a. Back up the configuration file in /etc, for example by entering the following command (Recommended):
   `cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak`

   b. Change to the Netflow directory:
   `cd <install_dir>/Netflow`

   where <install_dir> is the target directory for installing the Harvester: /opt/CA/NFA/ or a custom location

   c. Copy the snmpd.conf file in the Netflow directory to the /etc/snmp directory, overwriting the existing file:
   `cp -i snmpd.conf /etc/snmp`

   d. Confirm the overwrite operation when prompted.

   e. Verify that the configuration file is in place:
   `ls -l /etc/snmp/snmpd.conf`

   f. Verify that the configuration file has the correct permissions:
   `chmod 600 snmpd.conf`

3. Configure SNMP to start automatically on each boot by entering the following command:
   `chkconfig snmpd on`
4. Start the SNMP service in either of the following ways:
   - Enter the command:
     `service snmpd start`
   - Navigate to Services in the user interface, select snmpd, Start, then click Save.

     The SNMP service starts with the community name that is defined in the snmpd file.

# Synchronize System Time

Synchronize the system time among all servers that have CA Network Flow Analysis components installed.

For information about performing this procedure on Windows servers, see the related topics for:

- Windows Server 2008 R2 (see page 81)
- Windows Server 2003 (see page 82)

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Required | Windows Server 2003,<br>Windows Server 2008 R2 | All servers |

We also recommend that you synchronize the system time for any Linux servers in your deployment and and for the server that hosts your CA Performance Center instance.

## Synchronize System Time on Windows Server 2008 R2

Complete the steps in this topic on each Windows Server 2008 R2 in your deployment, unless the system time is synchronized automatically.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Right-click the date or time on the right edge of the taskbar and select 'Adjust date/time.'

   The Date and Time dialog opens.
3. Click the Internet Time tab.

4. Click 'Change settings.'

   The Internet Time Settings dialog opens.

5. Select the check box labeled 'Synchronize with an Internet time server.'
6. Select the server with which you want to synchronize. The default is time.windows.com.
7. Click 'Update Now.'

   The system time is synchronized with the selected server.

8. Click OK in the Internet Time Settings dialog.
9. Click OK in the Date and Time dialog.

**Note**: If you have collection devices in different time zones, set each device to its local time zone. Times are converted to Greenwich Mean Time (GMT).

## Synchronize System Time on Windows Server 2003

This topic describes how to use the Windows Time service to synchronize system time among Windows Server 2003 systems. The goal is to configure all of your Windows Server 2003 systems to match their clocks the same time source. For information about other time synchronization tools and methods, consult the Microsoft support site.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Enter the following command at a command prompt:

   ```
   net time /querysntp
   ```

   The command returns the name of the Simple Network Time Protocol (SNTP) server with which the system is configured to synchronize time.

   **Example Return Value:**

   ```
   The current SNTP value is: time.windows.com, 0x1
   The command completed successfully.
   ```

3. Enter the following command:

   ```
   net time /SETSNTP:NTPServer
   ```

   where:

   NTPServer = Name of the SNTP server that was returned from the previous query

   **Example Command:**

   ```
   net time /SETSNTP:time.windows.com
   ```

   The return value indicates whether the command completed successfully.

4. (Optional)Verify that the Windows Time service is set to start automatically.
   a. Select Start, Administrative Tools, Services.

      The Services window opens.

   b. Double-click Windows Time in the Services list.

      The Windows Time Properties window opens.

   c. Verify that the Startup type value is Automatic.

   d. If the value is not Automatic, choose Automatic from the Startup type list.

   e. Click OK.

   f. Close the Services window.
5. Restart the system.

# Update the List of Trusted Internet Sites

Add the NFA console server to the list of trusted internet sites, unless your browser security settings allow unrestricted access to internet sites. The process varies by browser. The following instructions are for Microsoft Internet Explorer 8.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2003,<br>Windows Server 2008 R2 | Standalone, Console |

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Launch Internet Explorer 8 on the NFA console server.
3. Click Tools, Internet Options.

   The Internet Options window opens.
4. Select the Security tab.
5. Click the Trusted Sites icon.
6. Click Sites.

   The Trusted Sites dialog opens.
7. Enter **https://localhost** in the "Add this Web site to the zone" field.
8. Click Add.

   Your change is saved and the site is added to the Websites list.

9. Exit:
    a. Click Close.

       The Trusted Sites dialog closes and you return to the Internet Options window.
    b. Click OK.

       The Internet Options window closes.

# Modify the Router Access Control Lists

We recommend that you configure the router access control lists (ACLs) to ensure that Harvesters can perform SNMP polling.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2003,<br>Windows Server 2008 R2 | Standalone, Harvester |

**Note:** If loopback interfaces source the flow packets, verify that CA Network Flow Analysis can access the IP addresses of those interfaces.

# Disable User Account Control (UAC)

We recommend that you disable User Account Control (UAC) on any Windows Server 2008 R2 system that is used as the standalone server or NFA console server. UAC is not fully supported for the current version of CA Network Flow Analysis. Enabling UAC on the standalone server or NFA console server can result in unexpected behavior.

**Note:** UAC is not applicable to Windows Server 2003 systems.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2008 R2 | Standalone, Console |

Follow these steps:

1. Log in as a user who is a member of the Administrators group.
2. Open the User Accounts window:
   a. Click Start, Control Panel.

      The Control Panel opens.

   b. Click User Accounts.

      The User Accounts window opens.
3. Click "Change User Account Control settings."

   The User Account Control Settings dialog opens.
4. Move the slider bar to the bottom "Never notify" level, if it is not already at this level.

   UAC is set to be disabled for all local accounts on the server.
5. Click OK.

   You return to the User Accounts tasks page.
6. Close the window.

# Reconfigure Trap Receivers

Four traps in ReporterAnalyzer 9.0.1 had conflicting Object Identifiers (OIDs). The conflicts could create problems with the trap receiver, which could not use the trap OID to determine which type of trap to process. The traps with conflicting OID values were:

- nfaTrafficProtocolToSDataEventStart: 1.3.6.1.4.1.4498.1.0.8
- nfaTrafficProtocolToSDataEventStop: 1.3.6.1.4.1.4498.1.0.9
- nfaTrafficFlowsDataEventStart: 1.3.6.1.4.1.4498.1.0.10
- nfaTrafficFlowsDataEventStop: 1.3.6.1.4.1.4498.1.0.11
- netQoSProcessStart: 1.3.6.1.4.1.4498.1.0.8
- netQoSProcessStop: 1.3.6.1.4.1.4498.1.0.9
- netQoSProcessDelayStart: 1.3.6.1.4.1.4498.1.0.10
- netQoSProcessDelayEnd: 1.3.6.1.4.1.4498.1.0.11

To resolve the overlap, the Harvester traffic traps have been moved to a new OID section, and the MIB has been rewritten to reflect this change. The updated MIB is on the NFA console server in the following directory: <install_path>\reporter\MIB. Use the following table to make any necessary updates to the values for processing the ReporterAnalyzer or CA Network Flow Analysis traps that you use.

If your trap receiver processes Watchdog traps only, you do not need to update any definitions.

**Note:** The highlighted table rows show OID values that have been updated.

| OID Name | Updated OID Value | Previous OID Value |
|---|---|---|
| nfaInterfaceChangeName | 1.3.6.1.4.1.4498.10.2.1 | 1.3.6.1.4.1.4498.1.1.1.1 |
| nfaInterfaceChangeState | 1.3.6.1.4.1.4498.1.1.1.2 | 1.3.6.1.4.1.4498.10.2.2 |
| nfaDataEventName | 1.3.6.1.4.1.4498.10.2.3 | 1.3.6.1.4.1.4498.1.2.1.1 |
| nfaDataEventInterface | 1.3.6.1.4.1.4498.10.2.4 | 1.3.6.1.4.1.4498.1.2.1.2 |
| nfaDataEventDirection | 1.3.6.1.4.1.4498.10.2.5 | 1.3.6.1.4.1.4498.1.2.1.3 |
| nfaDataEventStartTime | 1.3.6.1.4.1.4498.6.2.6 | 1.3.6.1.4.1.4498.1.2.1.4 |
| nfaDataEventStartTime | 1.3.6.1.4.1.4498.10.2.6 | 1.3.6.1.4.1.4498.1.2.1.4 |
| nfaDataEventDuration | 1.3.6.1.4.1.4498.10.2.7 | 1.3.6.1.4.1.4498.1.2.1.5 |
| nfaDataEventStopTime | 1.3.6.1.4.1.4498.10.2.8 | 1.3.6.1.4.1.4498.1.2.1.6 |
| nfaDataEventResetReason | 1.3.6.1.4.1.4498.6.2.9 | 1.3.6.1.4.1.4498.1.2.1.7 |
| nfaDataEventRouterAddress | 1.3.6.1.4.1.4498.10.2.10 | 1.3.6.1.4.1.4498.1.2.1.8 |

| OID Name | Updated OID Value | Previous OID Value |
|---|---|---|
| nfaDataEventIfIndex | 1.3.6.1.4.1.4498.10.2.11 | 1.3.6.1.4.1.4498.1.2.1.9 |
| nfaTrafficProtocol | 1.3.6.1.4.1.4498.10.2.12 | 1.3.6.1.4.1.4498.1.101.1.1 |
| nfaTrafficProtocolThreshold | 1.3.6.1.4.1.4498.10.2.13 | 1.3.6.1.4.1.4498.1.101.1.2 |
| nfaTrafficProtocolObserved | 1.3.6.1.4.1.4498.10.2.14 | 1.3.6.1.4.1.4498.1.101.1.3 |
| nfaTrafficProtocolToS | 1.3.6.1.4.1.4498.10.2.15 | 1.3.6.1.4.1.4498.1.102.1.1 |
| nfaTrafficProtocolToSValue | 1.3.6.1.4.1.4498.10.2.16 | 1.3.6.1.4.1.4498.1.102.1.2 |
| nfaTrafficProtocolToSThreshold | 1.3.6.1.4.1.4498.10.2.17 | 1.3.6.1.4.1.4498.1.102.1.3 |
| nfaTrafficProtocolToSObserved | 1.3.6.1.4.1.4498.10.2.18 | 1.3.6.1.4.1.4498.1.102.1.4 |
| nfaTrafficFlowsThreshold | 1.3.6.1.4.1.4498.10.2.19 | 1.3.6.1.4.1.4498.1.103.1.1 |
| nfaTrafficFlowsObserved | 1.3.6.1.4.1.4498.10.2.20 | 1.3.6.1.4.1.4498.1.103.1.2 |
| | | |
| netQoSEventName | 1.3.6.1.4.1.4498.1.3 | 1.3.6.1.4.1.4498.1.3 |
| netQoSProcessName | 1.3.6.1.4.1.4498.1.4 | 1.3.6.1.4.1.4498.1.4 |
| netQoSProcessID | 1.3.6.1.4.1.4498.1.5 | 1.3.6.1.4.1.4498.1.5 |
| netQoSServerAddress | 1.3.6.1.4.1.4498.1.6 | 1.3.6.1.4.1.4498.1.6 |
| netQoSResourceName | 1.3.6.1.4.1.4498.1.7 | 1.3.6.1.4.1.4498.1.7 |
| netQoSResourceID | 1.3.6.1.4.1.4498.1.8 | 1.3.6.1.4.1.4498.1.8 |
| netQoSProcessDelay | 1.3.6.1.4.1.4498.1.9 | 1.3.6.1.4.1.4498.1.9 |
| netQoSProcessDelayThreshold | 1.3.6.1.4.1.4498.1.10 | 1.3.6.1.4.1.4498.1.10 |
| netQoSResourceUtilization | 1.3.6.1.4.1.4498.1.11 | 1.3.6.1.4.1.4498.1.11 |
| netQoSResourceUtilizationThreshold | 1.3.6.1.4.1.4498.1.12 | 1.3.6.1.4.1.4498.1.12 |
| | | |
| nfaInterfaceChangeEvent | 1.3.6.1.4.1.4498.10.1.0.1 | 1.3.6.1.4.1.4498.1.0.1 |
| nfaTrafficProtocolDataEventStart | 1.3.6.1.4.1.4498.10.1.0.2 | 1.3.6.1.4.1.4498.1.0.6 |
| nfaTrafficProtocolDataEventStop | 1.3.6.1.4.1.4498.10.1.0.3 | 1.3.6.1.4.1.4498.1.0.7 |
| nfaTrafficProtocolToSDataEventStart | 1.3.6.1.4.1.4498.10.1.0.4 | 1.3.6.1.4.1.4498.1.0.8 |
| nfaTrafficProtocolToSDataEventStop | 1.3.6.1.4.1.4498.10.1.0.5 | 1.3.6.1.4.1.4498.1.0.9 |
| nfaTrafficFlowsDataEventStart | 1.3.6.1.4.1.4498.10.1.0.6 | 1.3.6.1.4.1.4498.1.0.10 |
| nfaTrafficFlowsDataEventStop | 1.3.6.1.4.1.4498.10.1.0.7 | 1.3.6.1.4.1.4498.1.0.11 |
| netQoSProcessStart | 1.3.6.1.4.1.4498.1.0.8 | 1.3.6.1.4.1.4498.1.0.8 |

| OID Name | Updated OID Value | Previous OID Value |
|---|---|---|
| netQoSProcessStop | 1.3.6.1.4.1.4498.1.0.9 | 1.3.6.1.4.1.4498.1.0.9 |
| netQoSProcessDelayStart | 1.3.6.1.4.1.4498.1.0.10 | 1.3.6.1.4.1.4498.1.0.10 |
| netQoSProcessDelayEnd | 1.3.6.1.4.1.4498.1.0.11 | 1.3.6.1.4.1.4498.1.0.11 |
| netQoSResourceEventStart | 1.3.6.1.4.1.4498.1.0.12 | 1.3.6.1.4.1.4498.1.0.12 |
| netQoSResourceEventEnd | 1.3.6.1.4.1.4498.1.0.13 | 1.3.6.1.4.1.4498.1.0.13 |

**Next:** Complete the configuration tasks in the *CA Network Flow Analysis Administrator Guide* section named "Initial Configuration."

# Configure Web Content Expiration

We recommend that you configure IIS to ensure that fresh web content is displayed. With the Expire Web Content Immediately setting enabled, the browser displays an updated page from the server rather than displaying content from a cache.

For the steps to configure web content expiration, see the related topics for:

- Windows Server 2008 R2 (see page 88)
- Windows Server 2003 (see page 89)

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2003, Windows Server 2008 R2 | Standalone, Console |

## Configure Web Content Expiration on Windows Server 2008 R2

Use the steps in this topic to configure web content expiration as recommended on a standalone server or NFA console server that is running Windows Server 2008 R2.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Select Start, Administrative Tools, Internet Information Services (IIS) 6.0 Manager.

   The Internet Information Services Manager window opens.

3. Display the options for expiring web content:
   a. Click the server name in the Connections pane.

      The server features are displayed.

   b. Double-click the HTTP Response Headers icon in the HTTP Features group.

      The window displays the current HTTP Response Headers.

   c. Click Set Common Headers in the Actions pane.

      The Set Common Headers dialog opens.
4. Select the following options:
   - "Expire Web content" check box
   - Immediately
5. Save your changes and exit:
   a. Click OK.

      The Set Common Headers dialog closes.

   b. Close the Internet Information Services Manager window.

## Configure Web Content Expiration on Windows Server 2003

Use the steps in this topic to configure web content expiration as recommended on a standalone server or NFA console server that is running Windows Server 2003.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Select Start, Administrative Tools, Internet Information Services (IIS) Manager.

   The Internet Information Services Manager window opens.
3. Display the options for expiring web content:
   a. Click the server name in the left pane.

      The server features are shown in the right pane.

   b. Right-click Web Sites in the right pane and select Properties.

      The Web Sites Properties dialog opens.

   c. Click the HTTP Headers tab.
4. Select the following options:
   - "Enable content expiration" check box
   - "Expire Immediately" radio button

5. Save your changes and exit:
   a. Click OK.

      The Web Sites Properties dialog closes.

   b. Close the Internet Information Services Manager window.

# Prevent False Positive Events

We recommend that you create an empty TrapConfiguration key in the Windows Registry to prevent the SNMP service from logging false positive events. This topic describes how to perform this step on a system that is running either Windows Server 2008 R2 or Windows Server 2003.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Recommended | Windows Server 2003, Windows Server 2008 R2 | All servers |

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Open a command prompt window.
3. Run the following command:

   ```
   reg add
   HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConf
   iguration
   ```

   If the command executes successfully, the return value is: "The operation completed successfully."

   The TrapConfiguration registry key is created in the following location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters.

# Configure the Recycle Bin

Optionally, configure the Recycle Bin to remove deleted files from the server immediately. The default behavior is for the system to save copies of deleted files in the Recycle Bin. This topic includes steps for Windows Server 2008 R2 and steps for Windows Server 2003.

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Optional | Windows Server 2003,<br>Windows Server 2008 R2 | All servers |

**Follow these steps on Windows Server 2008 R2:**

1. Log in as a user who is a member of the Administrators group.
2. Right-click the Recycle Bin icon on the desktop.
3. Select Properties from the menu.

   The Recycle Bin Properties dialog opens.
4. Select Local Disk (C:) on the General tab.
5. Select the option labeled "Don't move files to the Recycle Bin. Remove files immediately when deleted."
6. Click Apply.
7. Repeat steps 2 through 4 for each additional drive that you want to configure.
8. Click OK.

**Follow these steps on Windows Server 2003:**

1. Log in as a user who is a member of the Administrators group.
2. Right-click the Recycle Bin icon on the desktop.
3. Select Properties from the menu.

   The Recycle Bin Properties dialog opens.
4. Choose whether to configure all drives or configure each drive independently:
   - Configure drives independently:
     a. Select the drive to configure: Click the Local Disk (C:) tab.
     b. Select the option labeled "Do not move files to the Recycle Bin. Remove files immediately when deleted."
     c. Click Apply.
     d. Repeat steps A and B for each additional drive that you want to configure.

- Use one setting for all drives:

  Select the option labeled "Do not move files to the Recycle Bin. Remove files immediately when deleted.

5. Click OK.

# Disable Unneeded Services

Optionally, you can disable unnecessary services. This step is designed to help secure your servers.

For the steps and a list of services that you can delete, see the related topics for:

- Windows Server 2008 R2 (see page 92)
- Windows Server 2003 (see page 94)

| Required/Optional | Operating System | Servers to Configure |
|---|---|---|
| Optional | Windows Server 2003, Windows Server 2008 R2 | All servers |

## Disable Unneeded Services on Windows Server 2008 R2

If you want to disable unneeded services on Windows Server 2008 R2 systems in your deployment, use the steps and list in this topic.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Open the Services window: Select Start, Administrative Tools, Services.

   The Services window opens.
3. Right-click the following services and select Manual or Disabled.

   Do not select Stop or the services will restart whenever the server is rebooted.

| Windows 2008 R2 Services That You Can Disable | | |
|---|---|---|
| ■ Application Layer Gateway Service | ■ Application Management | ■ Certificate Propagation |
| ■ Distributed Link Tracking Client | ■ Distributed Transaction Coordinator | ■ DNS Client |
| ■ Function Discovery Resource Publication | ■ Human Interface Device Access | ■ IP Helper |

**Windows 2008 R2 Services That You Can Disable**

- Link-Layer Topology Discovery Manager
- Microsoft Iscsi Initiator Service
- Multimedia Class Scheduler
- Netlogon
- Network List Service
- Network Location Awareness
- Portable Device Enumerator Service
- Print Spooler
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Registry
- Resultant Set of Policy Provider
- Secondary Logon
- Smart Card
- Smart Card Removal Policy
- Special Administration Console Helper
- SSDP Discovery
- Tablet PC Input Service
- Telephony
- Volume Shadow Copy
- Windows Audio
- Windows Audio Endpoint Builder
- Windows CardSpace
- Windows Color System
- WinHTTP Web Proxy Auto-Discovery Service
- WMI Performance Adapter

## Disable Unneeded Services on Windows Server 2003

If you want to disable unneeded services on Windows Server 2003 systems in your deployment, use the steps and list in this topic.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Open the Services window: Select Start, Administrative Tools, Services.

   The Services window opens.
3. Right-click the following services and select Manual or Disabled.

   Do not select Stop or the services will restart whenever the server is rebooted.

**Windows 2003 Services That You Can Disable**

- Application Layer Gateway Service
- Application Management
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- DNS Client
- Function Discovery Resource Publication
- Human Interface Device Access
- Netlogon
- Network Location Awareness
- Print Spooler
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Registry
- Resultant Set of Policy Provider
- Secondary Logon
- Smart Card
- Special Administration Console Helper
- Telephony
- Volume Shadow Copy
- Windows Audio
- Windows Color System
- WinHTTP Web Proxy Auto-Discovery Service
- WMI Performance Adapter

# Chapter 8: Uninstalling CA Network Flow Analysis

The CA Network Flow Analysis 9.1.3 includes an option to uninstall the product, which you can use to remove CA Network Flow Analysis after an installation or upgrade.

**Notes:**

- The Uninstaller has no Undo option: Once you uninstall the software, you cannot restore the deleted files automatically.
- You should be able to install and uninstall the CA Network Flow Analysis software once or twice without incident. If you have ongoing problems, we recommend that you contact CA Support rather than continue to install and uninstall the software.

Do not use the Uninstall option if you have upgraded from CA NetQoS ReporterAnalyzer 9.0.1. To successfully reinstall the software in this case, you must first re-image the system.

This section contains the following topics:



## Uninstallation Prerequisites

Before you begin uninstalling the CA Network Flow Analysis software from a server, verify that the component is working properly.

Complete the following checks:

- Verify that you are not uninstalling software that has been upgraded from CA NetQoS ReporterAnalyzer 9.0.1. If you uninstall this type of upgrade, you will not be able to reinstall the software on the same server without re-imaging the server.
- Verify that the appropriate databases are present, as listed in the following table.

| Database | Location | Standalone | Harvesters | NFA Console |
|---|---|---|---|---|
| reporter | <install_path>\MySql51\data\ reporter | Yes | | Yes |
| harvester | <install_path>\MySql51\data\ harvester | Yes | Yes | |
| poller | <install_path>\MySql51\data\ poller | Yes | Yes | |

| Database | Location | Standalone | Harvesters | NFA Console |
|---|---|---|---|---|
| ReaperArchive15 | <install_path>\Netflow\datafiles\ ReaperArchive15 | Yes | Yes | |
| data_retention | <install_path>\MySql51\data\ data_retention | Yes | Yes | |
| ReaperArchive | <install_path>\Netflow\datafiles\ ReaperArchive | Yes | Yes | |

- Verify that the CA Network Flow Analysis services and MySQL are running, as listed in the following table:

| Service | Standalone | Harvester | Console | DSA (3-Tier) |
|---|---|---|---|---|
| CA NFA Collection and Poller Webservices (nfa_collpollws on Linux) | Yes | Yes | | |
| CA NFA Data Retention (nfa_dataretention on Linux) | Yes | Yes | | |
| CA NFA DNS/SNMP Proxies (nfa_proxies on Linux) | Yes | Yes | Yes | Yes |
| CA NFA DSALoader | | | | Yes |
| CA NFA File Server (nfa_filewebservice on Linux) | Yes | Yes | Yes (3-tier) | |
| CA NFA Harvester (nfa_harvester on Linux) | Yes | Yes | | |
| CA NFA Poller (nfa_poller on Linux) | Yes | Yes | | |
| CA NFA Pump | | | | Yes |
| CA NFA Reaper (nfa_reaper on Linux) | | Yes | | |
| CA NFA RibSource | Yes | | Yes | |
| NetQoS MySql51 | Yes | Yes | Yes | Yes |
| NetQoS NQMySql51 (nfa_mysqlCSE on Linux) | Yes | Yes | Yes | Yes |
| NetQoS Reporter Manager | Yes | | Yes | |
| NetQoS Reporter/Analyzer General Services | Yes | | Yes | |
| NetQoS Reporter/Analyzer Pump | Yes | | Yes | |

| Service | Standalone | Harvester | Console | DSA (3-Tier) |
|---|---|---|---|---|
| NetQoS Reporter/Analyzer Query Services | Yes | | Yes | |
| NetQoS Reporter/Analyzer Report | Yes | | Yes | |
| NetQoS Reporter/Analyzer Watchdog | Yes | | Yes | |

# Uninstall CA Network Flow Analysis

This topic describes how to uninstall the CA Network Flow Analysis software by using the Uninstaller. You also can uninstall the software from the Windows Add or Remove Programs window, where it is listed under the publisher CA Technologies, Inc.

**Follow these steps:**

1. Log in as a user who is a member of the Administrators group.
2. Back up your data and configuration files. For information about this step, see the *CA Network Flow Analysis Administrator Guide.*
3. Exit from all applications--with no exceptions.
4. Start the Uninstaller: Double-click the Uninstaller shortcut in <install_path>\Uninstall:
   - Standalone system: Double-click Uninstall Reporter shortcut to uninstall the NFA console first, then double-click the Uninstall Harvester shortcut to uninstall the Harvester.

     If you attempt to uninstall the Harvester software first, an error message opens.
   - Distributed deployment: Double-click Uninstall Reporter (NFA console server), Uninstall Harvester (Harvester server), or Uninstall DSA (DSA server).

   The Uninstall window opens.
5. Click Uninstall.

   The Uninstaller removes all of the program and data files, including the following CA Network Flow Analysis and MySQL elements:
   - Data
   - Services
   - Registry entries
   - Shortcuts, links, and aliases

- Most files
- Some directories

When the process is complete, the screen displays a list of the directories and files that were not deleted.

**Note:** Leave the file system undisturbed while uninstallation is in progress. Do not attempt to view the progress in Windows Explorer, for example.

Once the program finishes, the Uninstall Complete screen opens.

6. Click Done to close the Uninstall Complete screen.
7. Wait a few minutes to allow the helper process to finish the final cleanup.

   Some files are not deleted until this phase is finished. Once the final cleanup is finished, the Uninstaller itself is deleted.

**Notes:**

- The uninstallation log is at the root level of the original installation path. For example, the Harvester uninstallation log is at: <install_path>\Harvester_Uninstall_<timestamp>.txt.
- You may want to manually delete any CA Network Flow Analysis directories and files that are still present.
- If you make an unsuccessful attempt to reinstall the software, contact CA Support.

# Chapter 9: Troubleshooting

This section provides some troubleshooting tips for problems that are revealed by prerequisite tests. Prerequisite tests can generate warnings or failure notices. If you receive a warning, you can correct the problem immediately or after the installation or upgrade software runs. Failures must be corrected before you can continue. Most of the troubleshooting topics are for prerequisite failures.

**Note:** Many prerequisite tests rely on general indicators to identify problem areas. Passing a prerequisite test is not a guarantee that everything is configured properly. It is important to meet all of the server requirements, verify that supported versions of the required software are installed and complete all of the configuration tasks.

The following prerequisite tests are run:

| Test | Description | Warning or Upgrade/Install Failure | Server |
|---|---|---|---|
| Browser | Checks the Registry for a browser. Verify that a supported browser version is installed (see page 23). | Warning | Standalone<br>Distributed: NFA console |
| CA Network Flow Analysis (Invalid Version) | Verifies that the server has a version of CA Network Flow Analysis that is supported for the upgrade (see page 13). | Failure | All servers |
| Console Tool | Verifies that the Console tool (see page 100) has run successfully before the Harvester portion of the upgrade begins. | Failure | Standalone<br>Distributed: NFA console, Harvester (Windows) |
| DEP | Verifies that the winmgt service is running. Configure DEP as described in this guide. (see page 36) | Warning | Standalone<br>Distributed: NFA console, Harvester (Windows) |
| FIPS Algorithm Policy | Verifies that the FIPS Algorithm policy is not enabled (see page 101). | Verify automatic fix or Failure | Standalone<br>Distributed: NFA console |
| Flash Player | Checks the Registry for any version of Adobe Flash Player (see page 24). | Warning | Standalone<br>Distributed: NFA console |
| IIS Installed | Verifies that the wcsvc service is running. Install and configure IIS as described in this guide (see page 28). | Warning | Standalone<br>Distributed: NFA console |
| IIS Version | Checks the Registry for IIS version 7.0. | Warning | Standalone<br>Distributed: NFA console |

| Test | Description | Warning or Upgrade/Install Failure | Server |
|---|---|---|---|
| Java Version | Verifies that the supported version of the Java Runtime Engine (see page 102) is installed. | Failure | All servers |
| .NET 3.5 Version | Checks for .NET version 3.5 SP1. If .NET version 3.5 is found, turns on SP1. | Failure | Standalone<br>Distributed: NFA console |
| .NET 4.0 Version | Verifies that .NET version 4.0 is not installed. | Failure | Standalone<br>Distributed: NFA console |
| Service Control command | Verifies that the Windows System32 directory contains the sc.exe file (see page 103). | Failure | Standalone<br>Distributed: NFA console, Harvester (Windows) |
| SNMP | Verifies that the snmp service is running and the process ID is present. Configure SNMP on Windows servers (see page 32) and Linux servers (see page 42). | Warning | Standalone<br>Distributed: NFA console, all Harvesters |
| Windows 2003 Detected | Verifies that the server is running Windows Server 2008, not Windows Server 2003. | Failure | Standalone<br>Distributed: NFA console, Harvester (Windows), DSA |

This section contains the following topics:



# Console Table Tool Check Warning

When I click Next in the License Agreement screen in the Harvester upgrade program, an error message opens, which has the title:

"Console Table Tool Check Warning"

A check verified that the Console tool was not run successfully on the NFA console server. Before you start the Harvester upgrade program, you must run the Console tool.

The Console tool prepares for the Harvester upgrade:

- 9.0.1 Upgrade: The tool copies router and interface information and adds the DSA server IDs to the nqrptr settings table. The utility runs only if routers and interfaces are present.
- 9.1.x Upgrade: The tool enables the revision history to be recorded.

The upgrade cannot proceed until the tool has been run. If you run the tool and the "Console Table Tool Check Warning" message still appears, contact CA Support.

# FIPS Algorithm Policy Is Enabled

When I click Next in the License Agreement screen in the installation or upgrade program for the NFA console, a Pre-requisite Check Warning message opens, which includes the following text:

> "The FipsAlgorithmPolicy registry key for this system is set to enabled. If the following key is enabled, Windows will not allow certain algorithms to run..."

The error message opens because a system check found the FipsAlgorithmPolicy key in the Windows Registry, which indicates that the Federal Information Processing Standard (FIPS) 140 cryptographic standard is enabled. While this policy is enabled, the server can run only the cryptographic algorithms that have been submitted to and approved by the National Institute of Standards and Technology (NIST).

This restriction can cause problems connecting to databases through Open Database Connectivity (ODBC). Problems with CA Network Flow Analysis connectivity may result.

To disable the FipsAlgorithmPolicy Registry key, click OK in the Pre-requisite Check Warning message. The FIPS algorithm policy is disabled and does not restrict database connections.

# Invalid Version

When I click Next in the License Agreement screen in the upgrade program, an error message opens, which has the title:

> "Invalid Version"

The error message opens because a system check discovered that the current version of CA Network Flow Analysis software is not supported for upgrade . The upgrade program exits when you click OK to close the error message. Before you upgrade the CA Network Flow Analysis software, upgrade your current product software to a supported software version (see page 13).

# Java Is Not Installed

If you attempt to launch the installation or upgrade program on a server that does not have a supported version of the Java Runtime Engine (JRE), an error message opens. You must install a supported version of the JRE, before you can proceed.

The error message reads:

> "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

**Follow these steps:**

1. (Optional) Determine which JRE version the server is running:
   a. Enter the following command at a command prompt or in a terminal window:
   `java -version`
   The command returns the JRE version that is installed.
2. Download the appropriate JRE installation file to the installation server.
   **Note:** The appropriate JRE installation file is included in the ISO files from CA Support, which also contain the product installation or upgrade executable files.
3. (Windows) Run the JRE .exe installation file:
   a. Open the Run window: Select Start, Run.
   b. Specify the path and file name for the installation program in either of the following ways:
      - Click Browse and use the Browse window to locate and select the file.
      - Enter the path and the file name in the Open field.
      - Click OK.
   c. Follow the prompts to complete installation.
4. (Linux) Run the JRE .bin installation file:
   a. Navigate to the JRE .bin file location in a terminal window.
   b. Enter the following command:
   `./jre`
   The JRE installation program starts.
   c. Follow the prompts to complete installation.
5. (Optional) Repeat step 1 to verify that the JRE version is updated correctly.

# SC.exe Is Not Installed

When I click Next in the License Agreement screen of the installation or upgrade program, an error message opens, which begins with the following text:

> "sc.exe is not installed. The installer was unable to find "sc.exe" in the System32 folder."

A system check did not find the Service Control command (the sc.exe file) in the Windows/System32 directory. The Service Control command is used for communicating with the Service Controller during command line operations. If the file is missing, the installation or upgrade program exits.

The sc.exe file is included with the Windows Server software by default. To correct the problem, restore the missing sc.exe from your Windows Server installation software, Windows Resource Kit, or other resource.

# SNMP Is Not Enabled

When I click Next in the License Agreement screen of the installation or upgrade program, an SNMP warning message opens. The message reads:

> "Pre-requisite Check Warning The following issues were found: SNMP is not enabled. While not required before installation, some functionality may not work correctly if these are not addressed."

The SNMP warning message opens because the prerequisite check does not find that the snmpd daemon is running. You can correct the problem when the warning appears or you can proceed with the installation or upgrade. In any case, CA Network Flow Analysis will not run properly until you configure SNMP (see page 42) and make sure that the snmpd and snmptrapd daemons are running.

Use the following procedures to check the SNMP status on a Linux server.

**Follow these steps:**

1. (Optional) Enter the status command in a terminal window:
   `/etc/init.d/snmpd status`

   The command returns the process ID of the snmpd daemon. If the return text does not list a process ID for the snmpd daemon is not running.

2. (Optional) Check the status in the Service Configuration window:
   a. Open the Service Configuration window: Select System, Administration, Server Settings, Services.

      The Service Configuration window opens with the Background Services tab selected.

   b. Locate snmpd and snmptrapd in the service list.
   c. Check the status of these services:
      - Select snmpd and review the status message that is displayed.
      - Select snmptrapd and review the status message that is displayed.
   d. Close the Service Configuration window.

# Index

## G



## H



## I



## J



## L



## N



## O



## P



## R



## S

## T



## U



## W